UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERIA

MAESTRIA EN GESTIÓN ESTRATÉGICA DE TECNOLOGÍAS DE LA INFORMACIÓN

"PROPUESTA DE UN PLAN DE GESTIÓN DE RIESGOS Y GESTIÓN ÉTICA PARA EL DEPARTAMENTO DE TECNOLOGÍAS EN EL SECTOR EDUCATIVO"

Trabajo de titulación previo a la obtención del Título de Magíster en Gestión Estratégica de Tecnologías de la Información.

AUTOR:

Ing. Eduardo Ramón Bernal Alvear.

CI: 0103881371

DIRECTOR:

Ing. Diego Arturo Ponce Vásquez, PhD.

CI: 0101822609

CUENCA- ECUADOR

2017

Resumen

La infraestructura de Tecnologías de la Información (TI) en las Universidades Ecuatorianas se encuentra en constante evolución en respuesta a la demanda de alumnos y nuevos servicios tecnológicos ofertados. Uno de los más importantes desafíos en la administración de infraestructura de TI es la adecuada gestión de los riesgos tecnológicos como por ejemplo ataques informáticos o virus. El presente trabajo de investigación plantea un plan de gestión de riesgos para el departamento de tecnologías de una institución de educación superior. Además, se incluyó el análisis de relevancia de la gestión ética por parte del personal del departamento de TI y en su manejo gerencial. El alcance del estudio contempló las tres áreas típicas de un Departamento de TI: Servicios Informáticos, Sistemas de Información y Redes de Comunicaciones e Infraestructura. El plan de gestión de riesgos planteado está basado en recomendaciones de los estándares ISO/IEC 31000:2011 para la gestión de riesgos y los ISO 37001:2016, ISO 26000 para la gestión ética. El análisis de estas recomendaciones y la formulación de salvaguardas fueron elaboradas con la herramienta PILAR en base a la metodología MAGERIT y a través de encuestas a ingenieros de TI.

Palabras Clave: RIESGOS TECNOLÓGICOS, ÉTICA, ISO 31000, MAGERIT, ISO 26000, EDUCATIVO.

Abstract

Information technology (IT) infrastructure in Ecuadorian Universities is in constant evolution in response to the growing number of students and the offer of new IT services. One of the most relevant challenges of IT infrastructure management is to properly address technological risks such as cyber attacks and virus. The purpose of the present research is to develop a risk management plan for the IT department of higher education institutions. Furthermore, the relevance of ethics for the IT staff and management was analyzed. The scope of the study include the typical three IT units: Information services, Information systems, and Networking & Infrastructure. The developed risk management plan is based on recommendations of the standards: ISO/IEC 31000:2011 for risk management and ISO 37001:2016, ISO 26000 for the management of ethics. The analysis of these recommendations and the formulation of safeguards were developed based on the MAGERIT methodology and with the aid of the software tool PILAR and surveys to IT engineers.

Keywords: TECHNOLOGICAL RISKS, ETHICS, ISO 31000, MAGERIT, ISO 26000, EDUCATIONAL.

Tabla de contenido

Resumen 2

Abstract 3

Lista de tablas 8

Lista de figuras 9

Dedicatoria 12

Agradecimientos 13

Introducción 14

Justificación 16

Objetivo General 17

Objetivos Específicos 17

Alcance 18

Capítulo 1 20

Marco teórico de la metodología del modelo de Gestión de Riesgos tecnológicos y gestión ética para el Departamento de Tecnología en el área educativa 20

1.1 Gestión de Riesgos Tecnológicos 20

1.2 Estándar ISO 31000:2011 20

1.3 Implementación de la gestión del riesgo 22

1.3.1 Implementar el marco de referencia para gestionar el riesgo 22

1.3.2 Implementar el proceso para la gestión del riesgo 23

1.4 Proceso para la Gestión del Riesgo 23

1.4.1 Comunicación y Consulta 24

1.4.2 Establecimiento del Contexto 25
1.4.3 Valoración del Riesgo 27
1.4.4 Tratamiento del Riesgo 28
1.4.5 Monitoreo y Revisión 30
1.5 Metodología para la Gestión de Riesgos Tecnológicos 31
1.5.1 MAGERIT 32
1.5.2 PILAR 34
1.6 Gestión ética 35
1.7 ISO 26000 35
1.8 ISO 37001:2016 36
1.9 Matriz RACI 37
1.10 Uso de las normas, metodologías y herramientas en la Gestión del Riesgo 37
1.11 La Gestión de Riesgos en la Ley Ecuatoriana 38
Capítulo 2 40
Situación actual del Departamento de Tecnología en la gestión de riesgos y gestión ética 40
2.1 Situación actual 40
Misión 40
Funciones 40
2.2 Estructura del Departamento Tecnológico 41
2.2.1 Recomendaciones sobre la estructura 42

2.3 Procesos **43**

2.3.1 Procesos Transversales 44

2.3.2 Procesos de Servicios Informáticos 44

2.3.3 Procesos de Sistemas de Información 45

2.3.4 Procesos de Redes y Comunicaciones 45

2.4 Evaluación de la Situación actual **46**

Capítulo 3 ..... **50**

Desarrollo de la propuesta del plan de Gestión de Riesgos de Tecnologías de Información y gestión ética para el Departamento de Tecnología **50**

3.1 Proceso propuesto **50**

3.2 Establecimiento del Contexto **50**

3.3 Identificación del riesgo **52**

3.4 Matriz del riesgo **54**

3.5 Análisis del riesgo **60**

3. 6 Evaluación del riesgo **61**

3.7 Tratamiento del riesgo **67**

3.8 Monitoreo y revisión **76**

3.9 Comunicación y Consulta **77**

Capítulo 4 Plan de Contingencia. **78**

4.1 Definición Plan de Contingencia **78**

4.2 Componentes de un Plan de Contingencia **78**

4.3 Desarrollo del Plan de Contingencia. 80

4.3.1 Organización de los equipos....80

Caso de estudio....83

4.3.2 Fase de Alerta....83

4.3.3 Fase de Transición....85

4.3.4 Fase de Recuperación....87

4.3.5 Fase de vuelta a la normalidad....88

4.3.6 Fin de la contingencia....89

Conclusiones y Recomendaciones....91

Glosario de términos. 94

Bibliografía 98

ANEXOS 101

Anexo A. Formato de Encuesta para evaluar la Situación Actual....101

Anexo B. Valoración de las amenazas utilizando la herramienta PILAR....103

Anexo C. Proceso Gestión Riesgos. 104

Anexo D Integrantes Grupos Plan de Contingencia. 106

Anexo E. Procedimiento de Restauración. 108

Anexo F. Código de ética para los riesgos tecnológicos. 109

Anexo G. Fórmula para calcular la muestra. 112

Anexo H. Preguntas para elaborar el código y las responsabilidades éticas. 113

Lista de tablas

Tabla 1 Beneficios norma ISO 31000.....21

Tabla 2 Procesos para la Gestión de Riesgos.....24

Tabla 3 Acciones y Ventajas de la Comunicación.....25

Tabla 4 Nivel de Correspondencia de las Metodologías frente a los elementos de TI.....32

Tabla 5 Uso de Metodologías, Normas y Herramientas en la Gestión de Riesgos 38

Tabla 6 Matriz RACI de cargos propuesto para el Departamento de Tecnología.....43

Tabla 7 Ejemplo de FODA del Departamento de Tecnología.....51

Tabla 8 Clasificación de los Activos 53

Tabla 9 Calculo de los riesgos promedios por Activo. 57

Tabla 10 Valor de Criterio.....61

Tabla 11 Degradación y Probabilidad.....63

Tabla 12 Valoración de las amenazas.....63

Tabla 13 Valoración de las Salvaguardas y Responsabilidades éticas......68

Tabla 14 Actividades y Responsables del Plan de Contingencia 82

Tabla 15 Tipos de Desastres 84

Tabla 16 Equipos para ejecutar el PDC. 86

Tabla 17 Requerimiento Interno para el PDC.....87

Tabla 18 Requerimiento Externo para el PDC 89

Lista de figuras

Figura 1. La relación entre los principios de la gestión del riesgo 22

Figura 2. Implementar Marco de Referencia 23

Figura 3. Contexto Interno y Externo de la Organización. 26

Figura 4. Ciclo del Tratamiento del Riesgo 29

Figura 5. Marco de trabajo para la gestión de riesgos 33

Figura 6. Organigrama ejemplo del Departamento de Tecnología. 42

Figura 7. Resultados encuesta preguntas al Departamento de Tecnología por área. 47

Figura 8. Categorización de Activos con la herramienta PILAR. 52

Figura 9. Matriz del riesgo. 55

Figura 10. Activos por vulnerabilidad y por área. 60

Figura 11. Valoración de los activos. 62

Figura 12. Componentes fundamentales en el éxito del PDC. 80

Figura 13. Equipos para ejecutar el PDC. 85

Figura 14. Jerarquía de Dependencias de activos. 86

Universidad de Cuenca

Cláusula de Propiedad Intelectual

Eduardo Ramón Bernal Alvear, autor del trabajo de titulación "PROPUESTA DE UN PLAN DE GESTIÓN DE RIESGOS Y GESTIÓN ÉTICA PARA EL DEPARTAMENTO DE TECNOLOGÍAS EN EL SECTOR EDUCATIVO", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor.

Cuenca, 20 noviembre 2017

Eduardo Ramón Bernal Alvear

C.I: 0103881371

Universidad de Cuenca

Cláusula de licencia y autorización para publicación en el Repositorio Institucional

---

Eduardo Ramón Bernal Alvear en calidad de autor y titular de los derechos morales y patrimoniales del trabajo de titulación "PROPUESTA DE UN PLAN DE GESTIÓN DE RIESGOS Y GESTIÓN ÉTICA PARA EL DEPARTAMENTO DE TECNOLOGÍAS EN EL SECTOR EDUCATIVO", de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN reconozco a favor de la Universidad de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos.

Asimismo, autorizo a la Universidad de Cuenca para que realice la publicación de este trabajo de titulación en el repositorio institucional, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Cuenca, 20 noviembre 2017

Eduardo Ramón Bernal Alvear

C.I: 0103881371

Dedicatoria

Esta tesis la dedico en primer lugar a Dios por guiarme con su sabiduría y entendimiento para poder culminar de mejor manera mi proyecto.

A mi esposa Mayra e hijos Carlos y Alejandro que con su amor y comprensión me motivaron a seguir adelante compartiendo conmigo cada instante durante todo el trayecto convirtiéndose en el pilar fundamental para darme la confianza y llegar a la meta.

A mis Padres por la confianza apoyo y amor puesta en mí y a los que nunca defraudare.

Eduardo Bernal Alvear

Agradecimientos

Quiero agradecer a mi Dios y a mi familia por todo el apoyo brindado en todo momento para culminar con éxito mi proyecto.

A mi Director de tesis Ing. Diego Ponce PHD. que supo guiarme con sus consejos y recomendaciones valiosas como profesional.

Al Departamento de Tecnología de la Institución de educación superior, colegas y amigos que me abrieron sus puertas para juntos poder estructurar e investigar el tema desarrollado.

A la Universidad de Cuenca con sus Docentes que me supieron impartir sus conocimientos en el aula de clases.

A todos muchas gracias.

Eduardo Bernal Alvear

Introducción

En la actualidad, los Departamentos de Tecnología en el sector educativo, cuentan con diversos sistemas informáticos, infraestructura de redes, servicios informáticos, gran cantidad de información confidencial de los registros académicos de los estudiantes, servidores, bases de datos y demás activos tecnológicos tangibles e intangibles para dar soluciones oportunas a los usuarios y por motivos de confidencialidad no se dará el nombre de la institución. Sin embargo, el problema radica en la falta de prevención de riesgos tecnológicos contra vulnerabilidades en la seguridad de los datos que permita al departamento de tecnología actuar con ética y responsabilidad en el menor tiempo posible cuando el riesgo ocurra. Por lo antes mencionado, es necesario que el Departamento de Tecnología implemente un plan de gestión de riesgo y un plan de gestión ética, con el objetivo de tener una guía completa para prevenir los riesgos tecnológicos y cómo actuar en el momento de que estos ocurran, dando prioridad a los riesgos que generen el mayor impacto en la organización. Además, se debe tener presente el riesgo humano, por lo que es necesario tener un código de ética profesional que permita al personal, especialmente que labora en el departamento de tecnología, trabajar con responsabilidad bajo los lineamientos del comportamiento ético de la institución.

En este trabajo se aplica la metodología MAGERIT v3 (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012) con la herramienta PILAR (PILAR, 2017) para aplicar la norma ISO 31000:2011. La herramienta PILAR se centra para el caso de estudio en la implementación del proceso de gestión de riesgos tecnológicos, por otro lado, la norma ISO 26000 y 37010 son estándares para tratar el comportamiento ético del personal. Todo esto permitió la construcción de un Plan

de Gestión de Riesgos y un Código de ética para el Departamento de Tecnología en el sector educativo, y los resultados obtenidos podrán ser un referente para las demás áreas de la organización.

La tesis está organizada como sigue: Capítulo 1 Marco teórico de la metodología del modelo de Gestión de Riesgos Informáticos y gestión ética para el DT. En este capítulo se presenta un marco conceptual de la metodología, normas y mejores prácticas para la gestión de riesgos y gestión ética.

Capítulo 2 Situación actual del Departamento de Tecnología en la gestión de riesgos y gestión ética. Este capítulo tiene los antecedentes y analiza el estado actual de cómo se está llevando a cabo la Gestión de riesgos y la Gestión ética con el levantamiento de información mediante entrevistas en el Departamento Tecnológico.

Capítulo 3 Desarrollo de la propuesta del plan de Gestión de Riesgos de Tecnologías de Información y gestión ética para el DT. En este capítulo se desarrolla la metodología propuesta como resultado de las vulnerabilidades encontradas en el estudio de la situación actual y la mejor solución a ser implementada producto del análisis de las metodologías.

Capítulo 4 Plan de Contingencia. En este capítulo se presenta el desarrollo de un Plan de Contingencia de uno de los riesgos encontrados en la investigación y que tiene mayor impacto en la organización.

Y finalmente las conclusiones y recomendaciones para la Gestión de Riesgos y Gestión ética para el Departamento de Tecnologías.

Justificación

Los expertos del Foro Económico Mundial posesionan al riesgo tecnológico en el tercer lugar luego de los riesgos económicos y climáticos. Se asevera que el fraude o el robo de datos personales o profesionales ha alcanzado "niveles sin precedentes" y destacan entre los riesgos tecnológicos más probables en los próximos diez años “los ataques cibernéticos a gran escala” sexto lugar entre los diez primeros (Wyman, 2017).

Ante estas amenazas y debido a la gran cantidad de información y servicios informáticos que presta el DT, se tiene la necesidad de presentar una propuesta de gestión de riesgos que permita reducir el riesgo de un desastre informático y como mitigarlo en el caso de que ocurra con un plan de contingencia.

Para poder reducir o evitar los riesgos a nivel informático es necesario un correcto plan de gestión de riesgos de tecnologías que permita tener una guía práctica ya que existe mucha información, pero pocos casos de uso.

La propuesta de gestión de riesgos será entregada a el DT en un plazo no mayor de 5 meses, esta propuesta contendrá el plan de gestión de riesgos y de gestión ética y el plan de contingencia para el riesgo de mayor impacto con los debidos análisis y recomendaciones que cumplan con las normas internacionales de protección de riesgos y resaltar la importancia ética de gestionarlos con políticas de comportamiento ético. Ya que se puede tener un excelente plan de gestión de riesgos, pero si no existe la voluntad de gestionarlos con ética y responsabilidad no funcionará.

Con este plan de gestión de riesgos y ética se estima que se podría, reducir los niveles de servicio SLA en un 50% ante una posible catástrofe de los servicios que presta el DT hacia las

diferentes dependencias que conforman el sector educativo; con el único objetivo tener servicios informáticos más seguros y como recuperarlos en el menor tiempo posible en el caso de un desastre tecnológico. La información de los riesgos más críticos y de la ética se piensa obtener mediante el análisis de políticas y procesos, entrevistas a los Coordinadores de las tres áreas informáticas que está compuesta el DT, como también la opinión del personal técnico que lo conforman y de los usuarios administrativos que utilizan los servicios informáticos que presta el Departamento de Tecnologías.

Objetivo General

Identificar los principales riesgos tecnológicos en el DT en el sector educativo a fin de darles un tratamiento preventivo en conformidad a la norma ISO 31000:2011 (ISO, 2011); así también evidenciar la importancia de la gestión ética de la Gerencia y del personal que conforma el DT utilizando la norma ISO 37000/37001:2016 y 26000 (Argandoña & Isea, 2011).

Objetivos Específicos

Analizar la situación actual identificando los riegos que tengan un nivel más crítico y que afectan a los servicios que presta el DT, identificar a las partes involucradas para obtener la información mediante la utilización de entrevistas.

Analizar y evaluar las distintas metodologías que sirvan para poder elaborar el Plan de Gestión de riesgos y de Gestión ética para el Departamento de tecnologías.

Elaborar una propuesta de Gestión ética con políticas de conducta y de manejo de la organización.

Elaborar el plan de Gestión de riesgos, para esto se va a evaluar los tres riesgos de mayor criticidad en cada una de las tres áreas o coordinaciones con la utilización de la matriz de riesgos.

Entregar al DT la propuesta metodológica con el Plan de Gestión de riesgos y de Gestión ética, también se incluirá un plan de contingencia con uno de los riesgos de mayor criticidad para poder gestionar prevenir y monitorear de mejor manera los riesgos tecnológicos y éticos.

Alcance

En el presente estudio se pretende identificar la situación actual del Departamento de Tecnología para luego, analizar, evaluar, tratar y monitorear los riegos de mayor criticidad utilizando para ello la norma ISO 31000:2011 (ISO, 2011), así también evidenciar la importancia de la gestión ética de la alta Gerencia en el desarrollo de la propuesta utilizando para ello la norma ISO 37000/37001:2016/26000. Debido a la gran cantidad de riesgos que se puedan identificar, se tomarán los 2 o 3 más relevantes o los de mayor impacto hacia la organización por cada coordinación del DT; para evidenciar la importancia de la Gestión ética del manejo de la organización se tomará los puntos más relevantes que tengan que ver con el manejo de los riesgos de TI. Para poder cumplir con los estándares de las ISO 31000:2011 y 37001:2016 que habla de los riesgos y de la gestión ética respectivamente, también se realizara el plan de contingencia de uno de los riesgos tecnológico; que sea de mayor criticidad para la organización. Para todo esto es importante analizar y utilizar la información adecuada tales como políticas, procesos, manuales, COBIT, los estándares ISO y distinta bibliografía que aporten a conseguir la solución al problema planteado. Al finalizar, se entregará a el DT el

documento interno confidencial con la propuesta del plan de Gestión de riesgos y la importancia de la Gestión ética para la ejecución de la misma, se dejará abierta para que en un futuro se complete los demás riesgos encontrados, pero de menor relevancia.

Capítulo 1

Marco teórico de la metodología del modelo de Gestión de Riesgos tecnológicos y gestión ética para el Departamento de Tecnología en el área educativa

A continuación, se presenta un marco teórico de las normas, metodologías y mejores prácticas para la gestión de riesgos y gestión ética, se analizará la metodología que mejor cumpla con los requerimientos de la norma ISO 31000 y estándares internacionales para la Gestión de riesgos y la Gestión ética necesarias para el Departamento de Tecnología en el sector educativo. Para entender de mejor manera se va a trabajar con los siguientes conceptos.

1.1 Gestión de Riesgos Tecnológicos

El riesgo tecnológico puede incidir en las metas y objetivos de la organización y derivar en otro tipo de riesgo al ser intrínseco al uso de la tecnología. Por ello el daño, interrupción, modificación o falla derivada del uso de TI puede ocasionar pérdidas significativas en las organizaciones, las perdidas pueden ser financieras, multas o acciones legales, la afectación de la imagen de una organización y causar inconvenientes a nivel operativo y estratégico. (Ramírez Castro & Ortiz Bayona, 2011).

1.2 Estándar ISO 31000:2011

Son principios y directrices para ejecutar el proceso de gestión de riesgos. Puede ser utilizado por cualquier organización independientemente de su tamaño, actividad o sector.

"El uso de ISO 31000 puede ayudar a las organizaciones a incrementar la probabilidad de alcanzar los objetivos, mejorar la identificación de oportunidades y amenazas, asignar y utilizar recursos efectivamente para el tratamiento del riesgo". (ISO, 2011) Sin embargo, la ISO 31000 no es utilizada con fines de certificación, más bien ayuda en la orientación para el

levantamiento de auditoria tanto interna o externa. Las organizaciones que lo utilizan pueden verse beneficiadas al comparar sus prácticas de gestión de riesgos con un reconocimiento nacional o internacional, proporcionando principios eficaces para una gestión.

La norma ISO 31000:2011 habla sobre distintas clases de riesgos, por lo que se centrara el estudio del riesgo tecnológico específicamente en un Departamento de Tecnología.

Cuando la gestión del riesgo se implementa y se mantiene de acuerdo con esta norma, dicha gestión le permite a la organización, tener los siguientes beneficios:

Tabla 1
Beneficios norma ISO 31000

Aumentar la probabilidad de alcanzar los objetivos.
Fomentar la gestión proactiva.
Ser consciente de la necesidad de identificar y tratar los riesgos en toda la organización.
Cumplir con los requisitos legales y reglamentarios pertinentes y con las normas internacionales.
Mejorar la presentación de informes obligatorios y voluntarios.
Mejorar el gobierno.
Mejorar la confianza y honestidad de las partes involucradas. (Gestión ética).
Establecer una base confiable para la toma de decisiones y la planificación.
Mejorar los controles.
Asignar y usar eficazmente los recursos para el tratamiento del riesgo.
Mejorar la eficacia y la eficiencia operativa.
Mejorar la prevención de pérdidas y la gestión de incidentes.
Minimizar las pérdidas.
Mejorar el aprendizaje organizacional.
Mejorar la flexibilidad organizacional.

Nota: Beneficios para las organizaciones cuando se implementa la norma ISO 31000
Fuente: (NTE-INEN-ISO 31000, 2014) (Elaboración Propia).

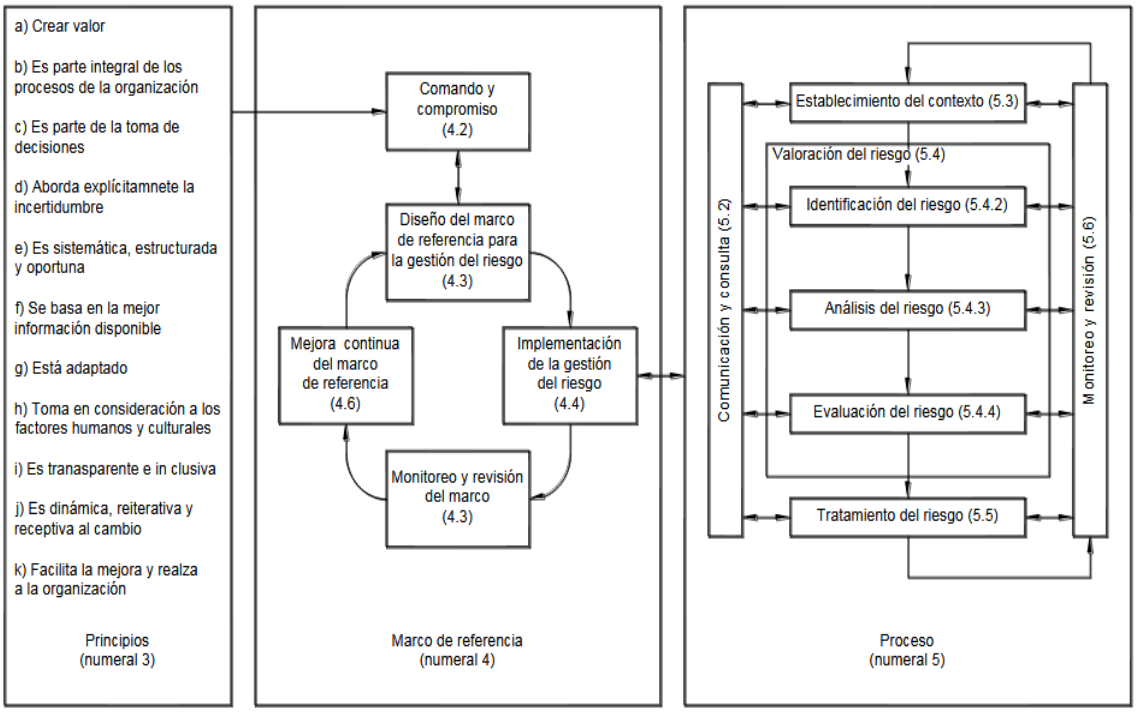


Figura 1. *La relación entre los principios de la gestión del riesgo*
El marco en el que se produce el proceso de la gestión de riesgo. Fuente: (ISO, 2011)

El marco de referencia como se muestra en la Figura 1. puede ser un tema orientado hacia la organización. Para el caso de estudio se va a trabajar en la implementación o proceso de la gestión del riesgo tecnológico.

1.3 Implementación de la gestión del riesgo

En esta etapa se debe asociar dos tipos de implementación la de la Organización con el marco referencial, según COBIT para cumplir con la Gestión del riesgo una alta Gerencia debe involucrarse en la toma de decisiones. Por otra parte, el Departamento de Tecnología es el que debe implementar del proceso de la Gestión del riesgo.

1.3.1 Implementar el marco de referencia para gestionar el riesgo

La organización para la implementación del marco de referencia se debería realizar los siguientes aspectos:

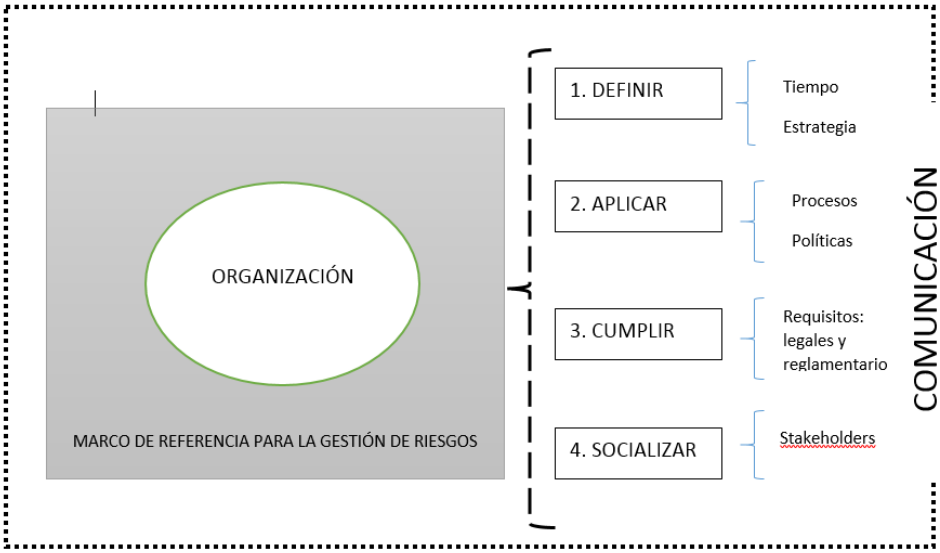


***Figura 2**. Implementar Marco de Referencia*
Fuente: (Elaboración Propia) & (NTC-ISO 31000, 2011)

1.3.2 Implementar el proceso para la gestión del riesgo

La gestión del riesgo se debería implementar garantizando que el proceso para la gestión del riesgo que se describe en la Tabla 2, se aplica a través de un plan para la gestión del riesgo en todos los niveles y las funciones pertinentes de la organización como parte de sus prácticas y procesos. (NTC-ISO 31000, 2011) .

1.4 Proceso para la Gestión del Riesgo

El proceso para la gestión del riesgo debería:

- Ser parte integral de la gestión.
- Estar incluido en la cultura o responsabilidad ética y las prácticas.
- Estar adaptado a los procesos de negocio de la organización.

El proceso comprende las actividades que se describen en los numerales 5.2 al 5.6. de la Figura 1. El proceso para la gestión del riesgo se ilustra en la Tabla 2. Que muestra el detalle de cada proceso para implementar la gestión del riesgo.

Tabla 2
Procesos para la Gestión de Riesgos

Proceso	Descripción
Comunicación y Consulta	Comprende definir y utilizar mecanismos para comunicar y consultar con los interesados internos y externos, según resulte apropiado en cada etapa del Proceso de Gestión de Riesgos
Evaluación del Riesgo:	Identificación del Riesgo: Proceso de búsqueda, reconocimiento y descripción de riesgos. Comprende identificar los riesgos y las oportunidades que puedan contribuir al logro de los referidos objetivos. Análisis del Riesgo: Proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo. El análisis del riesgo proporciona las bases para la valoración del riesgo y para tomar las decisiones relativas al tratamiento del riesgo. Valoración del Riesgo: Proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.
Tratamiento del Riesgo	Involucra la selección y el acuerdo para aplicar una o varias opciones pertinentes para cambiar la probabilidad de que los riesgos ocurran, los efectos de los riesgos, o ambas, y la implementación de estas opciones.
Monitoreo y Revisión	Comprende definir y utilizar mecanismos para la verificación, supervisión, observación crítica o determinación del estado de los riesgos y controles.

Nota: Pasos para el proceso de la Gestión de Riesgos
Fuente: (NTC-ISO 31000, 2011) (Elaboración propia).

La norma ISO 31000:2011 describe los lineamientos que debe seguir cada una de las etapas que contiene el Proceso para la Gestión de Riesgos que se detallan a continuación:

1.4.1 Comunicación y Consulta

La comunicación y consultas se deben realizar con todas las partes involucradas internas y externas siendo de forma transversal durante todas las etapas del proceso de gestión del riesgo. (NTC-ISO 31000, 2011)

Tabla 3
Acciones y Ventajas de la Comunicación

Responsable	**Acciones/ Herramientas**	**Ventajas**
Equipo Gestor de riesgos y Seguridad	Establecer contexto	Ayudar a definir el alcance de la Gestión de riesgos
	Identificar los riesgos	Garantizar que todos los riesgos este identificados
	Intereses de la partes involucradas	Garantizar que se entiende y se toma en consideración las opiniones de los involucrados.
	Reunir las áreas	Garantiza los riesgos con las opiniones de los expertos
	Plan de Tratamiento	Asegurar la aprobación y el soporte del riesgo que se va a tratar
	Gestión de Cambios	Identificar los cambio necesarios del Plan de Gestión
	Plan de Comunicación	Mantener informado a los involucrados internos y externos

Fuentes: (Elaboración Propia) & (NTC-ISO 31000, 2011)

1.4.2 Establecimiento del Contexto

Define parámetros tanto internos como externos de los objetivos de la Organización.

1.4.2.1 Establecer el contexto externo

Para entender el contexto externo es importante que se tomen en consideración todas las percepciones y valores de las partes involucradas externas en el ambiente social, cultural tanto nacional como internacional. (NTC-ISO 31000, 2011)

1.4.2.2 Establecer el contexto interno

El contexto interno es el ambiente interno en el cual la organización busca alcanzar sus objetivos. El proceso para la gestión del riesgo debería estar alineado con la cultura, los procesos, la estructura y la estrategia de la organización. Para entender mejor el contexto interno y externo de la Gestión del Riesgo con respecto a la organización este se detalla en la siguiente figura.

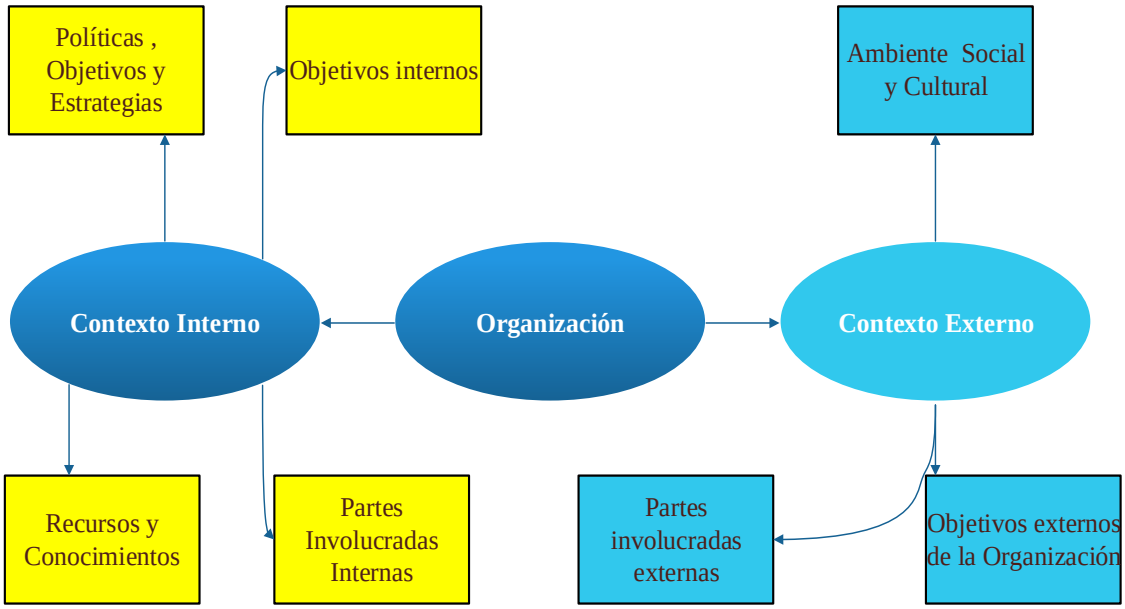


Figura 3. *Contexto Interno y Externo de la Organización.*
Fuente: (Elaboración Propia) & (NTC-ISO 31000, 2011)

1.4.2.3 Establecer el contexto del proceso para la gestión del riesgo

El contexto del proceso para la gestión del riesgo variará de acuerdo con las necesidades de la organización.

Este contexto puede involucrar, entre otros:

- Definición de las actividades, las metas y los objetivos de gestión del riesgo.
- Definición de las responsabilidades del proceso.
- Definición del alcance, así como de la profundidad y extensión de las actividades de gestión del riesgo con exclusiones e inclusiones.

- Definir tiempo y ubicación de la actividad, proceso, función, proyecto, producto, servicio o activo.
- Definición de las relaciones entre el proyecto, el proceso o la actividad particulares y otros proyectos, procesos o actividades de la organización.
- Definición de las metodologías para la valoración del riesgo.
- Definición de la forma de evaluar el desempeño y la eficacia en la gestión del riesgo.
- Identificación y especificación de las decisiones que se deben tomar (NTC-ISO 31000, 2011).

1.4.2.4 Definir los criterios del riesgo

La organización debería definir los criterios que se van a utilizar para evaluar la importancia del riesgo, los factores que se van a considerar deberían incluir los siguientes:

- La naturaleza y los tipos de causas y consecuencias y como se van a medir.
- Cómo se va a definir la probabilidad.
- Cómo se va a determinar el nivel de riesgo.
- Las partes involucradas con sus puntos de vista.
- El nivel en el cual el riesgo se torna aceptable o tolerable.
- La Dependencia o combinación de riesgos múltiples. (NTC-ISO 31000, 2011)

1.4.3 Valoración del Riesgo

La valoración de los riesgos es el proceso total de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

1.4.3.1 Identificación del Riesgo

La organización debería identificar las fuentes de riesgo, las áreas de impacto, los eventos y sus causas y consecuencias potenciales. Generando una lista de riesgos que podrían retrasar los logros de la Organización

Es importante identificar la totalidad de los riesgos asociados, riesgo que no se identifique en esta fase no será incluido en el análisis posterior.” (NTC-ISO 31000, 2011).

1.4.3.2 Análisis del Riesgo

El análisis del riesgo ayuda en la comprensión del riesgo. Con el análisis se determina si es necesario tratar o no el riesgo y sobre las estrategias y métodos más adecuados para su tratamiento. El análisis del riesgo brinda una entrada para la toma de decisiones, en la cual se deben hacer elecciones y las opciones implican diversos tipos y niveles de riesgo. (NTC-ISO 31000, 2011)

1.4.3.3 Evaluación del Riesgo

La evaluación permite la toma de decisiones, basada en los resultados de dicho análisis, para poder dar el tratamiento en base a su prioridad (NTC-ISO 31000, 2011)

1.4.4 Tratamiento del Riesgo

El tratamiento del riesgo proporciona controles o trata de modificar el riesgo. El tratamiento del riesgo implica un proceso cíclico como se muestra en la siguiente figura.

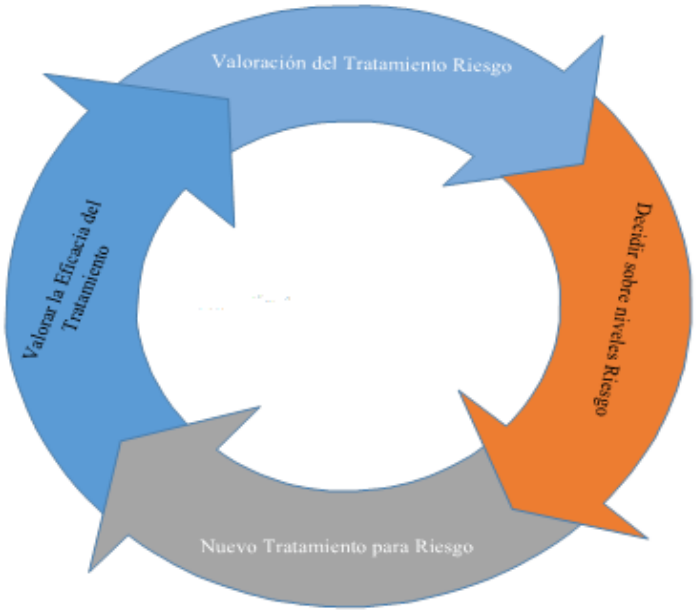


Figura 4. *Ciclo del Tratamiento del Riesgo*
Fuente: (Elaboración Propia) & (NTC-ISO 31000, 2011)

Las opciones para el tratamiento del riesgo no necesariamente son mutuamente excluyentes ni adecuadas en todas las circunstancias.

Las opciones pueden incluir las siguientes:

a) Evitar el riesgo al decidir no iniciar o continuar la actividad que lo originó;
b) Tomar o incrementar el riesgo para perseguir una oportunidad;
c) Retirar la fuente de riesgo;
d) Cambiar la probabilidad;
e) Cambiar las consecuencias;
f) Compartir el riesgo con una o varias de las partes, (incluyendo los contratos y la financiación del riesgo); y
g) Retener el riesgo mediante una decisión informada. (NTC-ISO 31000, 2011)

1.4.4.1 Selección de las opciones para el tratamiento del riesgo

La selección de las opciones más adecuadas para el tratamiento del riesgo implica equilibrar el costo beneficio con respecto a los requisitos reglamentarios y legales. En las decisiones también se deberían considerar los riesgos que pueden ameritar el tratamiento que no es

justificable en términos económicos, por ejemplo, los riesgos graves (consecuencia negativa alta) pero raros (baja probabilidad).

Al seleccionar las opciones, la organización debería considerar los valores y las percepciones de las partes involucradas.

El plan de tratamiento debería identificar claramente el orden de prioridad en el cual se deberían implementar los tratamientos individuales para el riesgo.

El monitoreo es parte integral del plan de tratamiento del riesgo para garantizar la eficacia de las medidas que se están tomando.” (NTC-ISO 31000, 2011)

1.4.4.2 Preparación e implementación de los planes para el tratamiento del riesgo

“El propósito de los planes para el tratamiento del riesgo es documentar la forma en que se van a implementar las opciones de tratamiento seleccionadas.

La información suministrada en los planes de tratamiento debería incluir:

- Las razones para la selección de las opciones de tratamiento, que incluyan los beneficios que se espera obtener;
- Aquellos que son responsables de aprobar el plan y los responsables de implementarlo;
- Acciones propuestas;
- Requisitos de recursos, incluyendo las contingencias;
- Medidas y restricciones de desempeño;
- Requisitos de monitoreo y reporte; y
- Tiempo y cronograma.

Los planes de tratamiento se deberían integrar con los procesos de gestión de la organización y del código de ética importante en el manejo del personal involucrado.” (NTC-ISO 31000, 2011)

1.4.5 Monitoreo y Revisión

El monitoreo en la planificación y verificación del proceso de Gestión debe ser con regularidad y constantemente según sea necesario. Los responsables del monitoreo deberían ser claramente definidos.

Los procesos de monitoreo y revisión de la organización deberían comprender todos los aspectos del proceso para la gestión del riesgo con el fin de:

- Garantizar que los controles son eficaces y eficientes tanto en el diseño como en la operación.
- Obtener información adicional para mejorar la valoración del riesgo.
- Analizar y aprender lecciones a partir de los eventos (incluyendo los cuasi accidentes), los cambios, las tendencias, los éxitos y los fracasos.
- Detectar cambios en el contexto externo e interno, incluyendo los cambios en los criterios del riesgo y en el riesgo mismo que puedan exigir revisión de los tratamientos del riesgo y las prioridades.
- Identificar los riesgos emergentes. (NTC-ISO 31000, 2011)

1.5 Metodología para la Gestión de Riesgos Tecnológicos

Existen muchas metodologías que ayudan en la implementación de la Gestión de Riesgos Tecnológicos, los principales son:

OCTAVE Metodología del SEI (Software Engineering Institute) que considera tanto los temas organizacionales como los técnicos, también examina como la gente emplea la infraestructura en su trabajo diario. “El objetivo de OCTAVE es el riesgo organizacional y el foco son los temas relativos a la estrategia y a la práctica”. (Heredero, 2006)

CRAMM Basado en la ISO 27001 se orienta a que los responsables de la seguridad estén en condiciones, “bien de evitar o aceptar riesgos individuales o bien en reducir los riesgos a aceptables”. (Calle , 1996)

Risk IT Es una metodología de ISACA que ahorra tiempo, costos y esfuerzos al brindar un método claro para concentrarse en los riesgos comerciales relacionados con la tecnología de la información.

Tabla 4

Nivel de Correspondencia de las Metodologías frente a los elementos de TI

Mejor Practica	Elementos de TI							
	Hardware	Software	Bases de Datos	Redes y Telecomunicaciones	Recursos Humanos	Legal	Financiero	Servicios
OCTAVE	2	2	2	2	2	0	0	1
CMMI	1	2	2	1	1	0	0	1
RISK IT	2	2	2	2	2	1	1	2
MAGERIT	2	2	2	2	2	2	2	2

Nivel Correspondencia: 0 Bajo, 1 Medio, 2 Alto.

Fuente: (Carrillo, 2013) (Elaboración propia).

La metodología de OCTAVE se centra en las vulnerabilidades organizativas y tecnológicas (Espinoza, Martínez, & Siler, 2014) por otra parte MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

1.5.1 MAGERIT

"Siguiendo la terminología de la normativa ISO 31000, MAGERIT responde a lo que se denomina "Proceso de Gestión de los Riesgos", ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos". En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los

órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.” (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Para la implementación del proceso de gestión de riesgos utilizando MAGERIT se basa en tres libros.

Libro I: Método.

Libro II: Catálogo de elementos.

Libro III: Guía de Técnicas.

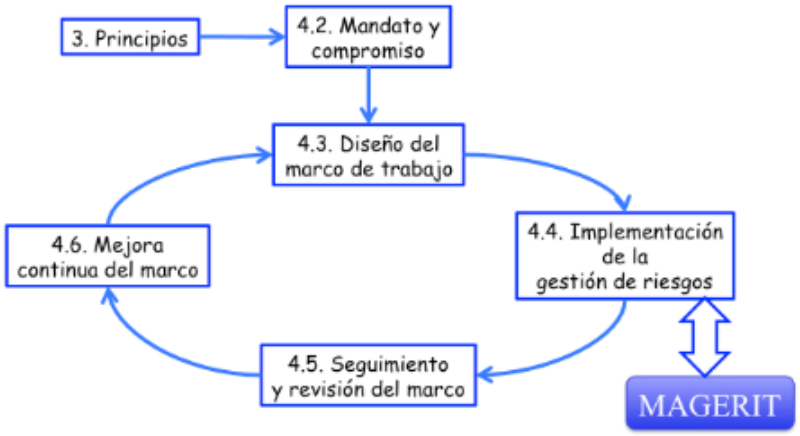


Figura 5. *Marco de trabajo para la gestión de riesgos*
MAGERIT actúa en la implementación de la Gestión del Riesgo Fuente: MAGERIT. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Se analizaron varios casos en donde se aplicó exitosamente la gestión de riesgos tecnológicos utilizando la metodología MAGERIT en el sector educativo. Uno de estos casos es la Escuela Superior Politécnica del Litoral, donde MAGERIT se utilizó para conocer las amenazas a los cuales se encuentran expuestos los activos que forman parte del departamento de informática de la ESPOL, mediante un análisis de riesgos de orden cualitativo se analizó el

nivel de madurez en la seguridad aplicada en la institución para finalmente sugerir las salvaguardas necesarias para reducir los niveles de riesgo e impacto. (Miranda, 2015). Otro caso es el aplicado a la zona pesquera e idustrial Bravito S.A. en la ciudad de Machala se utiliza MAGERIT utilizando procedimientos que son aplicados con la única finalidad de proteger un sistema de información perteneciente a una organización, previniendo ataques para minimizar riesgos. (Gaona, 2013)

El estado Ecuatoriano a traves de su Secretaria Nacional de Gestión de Riesgos en conjunto con el Ministerio de Educación a elaborado un Plan Institucional de Emergencias para Centros Educativos que se centra en los riesgos de origen natural, socionatural y antrópica. (Secretaria Nacional de Gestión de Riesgos, 2012) desde el punto de vista informático este Plan estaría incompleto ya que se deberia contemplar el riesgo tecnológico.

1.5.2 PILAR

La herramienta PILAR se va a utilizar para la implementación de MAGERIT en el Departamento de Tecnología del sector educativo.

"Es una herramienta desarrollada bajo especificación del Centro Nacional de Inteligencia para soportar el análisis de riesgos de sistemas de información siguiendo la metodología MAGERIT" (PILAR, 2017).

La herramienta soporta todas las fases del método MAGERIT:

- Caracterización de los activos: identificación, clasificación, dependencias y valoración.
- Caracterización de las amenazas
- Evaluación de las salvaguardas

La herramienta incorpora los catálogos del "Catálogo de Elementos" permitiendo una homogeneidad en los resultados del análisis

- Tipos de activos.
- Dimensiones de valoración.
- Criterios de valoración.
- Catálogo de amenazas. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

1.6 Gestión ética

Según COBIT 5 (2012) describe a la gestión ética como "al conjunto de conductas individuales y colectivas dentro de una empresa. La ética puede ser:

- Éticas Organizativas.
- Éticas Individuales.

Ética organizativa, determinada por los valores por los cuales la empresa quiere subsistir.

Éticas individuales, determinada por los valores personales de cada individuo dentro de la empresa y dependiendo de un importante grado de factores externos tales como religión, origen étnico, antecedentes socioeconómicos, geografía y experiencias personales."

1.7 ISO 26000

El tercer principio de la ISO 26000 es el comportamiento ético.

La Responsabilidad Social y la ética tienen mucho que ver con el comportamiento humano. Es por eso que la norma ISO 26000 propone que, la Organización debería regirse con criterios de equidad, honestidad e integridad para tener un impacto positivo en su interior y hacia la sociedad, lo que significa que la empresa para alcanzar un beneficio económico debe preocuparse en maximizar los impactos positivos en un entorno social, moral y minimizando la corrupción para mejorar la calidad del servicio. (Argandoña & Isea, 2011)

1.8 ISO 37001:2016

"La recientemente publicada ISO 37001, es una norma internacional de Sistemas de Gestión contra el soborno para la cual se ha tomado como base la norma ya existente BS 10500: Anticorrupción y Ética empresarial desarrollada por el British Standard Institute (BSI).

ISO 37001, especifica las medidas que la organización debe adoptar para evitar prácticas de soborno, ya sean de tipo directo o indirecto, por parte de su personal o socios de negocios que actúen en beneficio de la organización o en relación con sus actividades." (ISACA , 2016)

Estas medidas incluyen, entre otras:

- Adopción de una política anti-soborno.
- Nombramiento de una persona o conjunto de personas encargadas de supervisar el correcto funcionamiento del sistema de gestión para controlar su incumplimiento.
- Evaluación de los riesgos y debida diligencia en proyectos y socios de negocios.
- Aplicación de controles financieros y comerciales.
- Procedimientos de información e investigación.

Un caso práctico y que está ligado al procedimiento de adquisición de bienes Universitarios es el Sistema de Contratación Pública SERCOP manifiesta lo siguiente "El SERCOP se encuentra muy por encima de los parámetros mínimos que la ISO 37001 exige". Uno de los puntos a destacar es la existencia de matrices de riesgos, controles, monitoreo y seguimiento interno y externo de los procedimientos. Se destaca, por ejemplo, la existencia de una normativa que prohíbe la entrega de regalos, donaciones o dádivas por parte de los proveedores a las entidades contratantes.

1.9 Matriz RACI

La matriz RACI es también conocida como matriz de responsabilidades porque sirve para establecer las responsabilidades de cada actor que participa en una tarea. La matriz se construye con una tabla donde por filas tenemos tareas y por columnas actores.

En la intersección de cada fila con cada columna vamos colocando la responsabilidad de cada uno de estos roles: "R", "A", "C" o "I". Veamos el significado de las siglas. (ISACA, 2012).

- **"R" – Responsable** *del inglés Responsabile*. Es el rol encargado de realizar la tarea. Hay que tener cuidado que en este caso responsable significa responsable de realizar el trabajo
- . **"A" – Aprobador** *del inglés Accountable y algunas veces Approver*. Es el rol que aprueba el trabajo realizado por el Responsable.
- **"C" – Consultado** *del inglés Consulted*. Son aquellas personas que son consultadas sobre la cuestión, personas a las cuales se les pregunta su opinión sobre algún aspecto de la tarea ya bien sea porque deben tenerse en cuenta o porque son expertos en la materia.
- **"I" – Informado** *del inglés Informed*. Son aquellas personas a las que hay que mantener informadas sobre la evolución de la tarea. Lo más frecuente es informar de cuando se ha completado la tarea, pero dependiendo del rol y de la implicación pueden solicitar que se les informe de la evolución.

1.10 Uso de las normas, metodologías y herramientas en la Gestión del Riesgo

Para poder presentar la propuesta de este trabajo se utilizaron distintas normas, metodologías y herramientas con aportes del autor acoplándose a las necesidades de la institución como se muestra en la Tabla 5:

Tabla 5

Uso de Metodologías, Normas y Herramientas en la Gestión de Riesgos

Actividades	ISO/METODOLOGÍAS/HERRAMIENTAS									
	ISO 31000:2011	ISO 26000:2017	ISO 37001	ISO 27001:2013	MAGERIT	PILAR	COBIT 5	Entrevistas y Lluvia de Ideas	Políticas	Procesos
Recolección de Información								x	x	x
Identificación del Riesgo	x				x	x				x
Análisis del Riesgo	x				x	x				x
Evaluación del Riesgo	x				x	x				x
Tratamiento del Riesgo	x	x	x		x	x				x
Monitoreo y Revisión	x				x	x				x
Evaluación de la Situación Actual								x	x	x
Gestión ética		x	x						x	
Matriz RACI							x			
Matriz de Riesgos	x				x	x	x			x
Plan de Contingencia				x			x	x		x

Nota: Usos de metodologías, normas y herramientas en las actividades de la investigación Fuente: (Elaboración Propia).

1.11 La Gestión de Riesgos en la Ley Ecuatoriana

La Secretaría de Gestión de Riesgos en su Resolución Nro. SGR-029-2015 el artículo 3 del Reglamento a la Ley de Seguridad Pública y del Estado, establece que la Secretaría de Gestión de Riesgos es el órgano rector y ejecutor del Sistema Nacional Descentralizado de Gestión de Riesgos. Dentro del ámbito de su competencia le corresponde: *"a) Identificar los riesgos de orden natural o antrópico, para reducir la vulnerabilidad que afecten* o *puedan afectar al territorio ecuatoriano; b) Generar y democratizar el acceso y la difusión de información suficiente y oportuna para gestionar adecuadamente el riesgo* ***c) Asegurar que las instituciones públicas y privadas incorporen obligatoriamente, en forma transversal, la gestión de riesgo en su planificación y gestión;*** *d) Fortalecer en la ciudadanía y en las entidades públicas y privadas capacidades para*

identificar los riesgos inherentes a sus respectivos ámbitos de acción; e) Gestionar el financiamiento necesario para el funcionamiento del Sistema Nacional Descentralizado de Gestión de Riegos y coordinar la cooperación internacional en este ámbito; f) Coordinar los esfuerzos y funciones entre las instituciones públicas y privadas en las fases de prevención, mitigación, la preparación y respuesta a desastres, hasta la recuperación y desarrollo posterior; g) Diseñar programas de educación, capacitación y difusión orientados a fortalecer las capacidades de las instituciones y ciudadanos para la gestión de riesgos; y, h) Coordinar la cooperación de la ayuda humanitaria e información para enfrentar situaciones emergentes y/o desastres derivados de fenómenos naturales, socio naturales o *antrópicos a nivel nacional e internacional".* (Secretaría Gestión de Riesgos, 2015)

Capítulo 2

Situación actual del Departamento de Tecnología en la gestión de riesgos y gestión ética

2.1 Situación actual

La Organización para el presente estudio es una Institución del Sector Educativo localizada en la ciudad de Cuenca provincia del Azuay, y se enfocó el análisis en el Departamento de Tecnologías. Debido a políticas de seguridad y confidencialidad no se dará el nombre de la institución, todos los nombres de responsables involucrados en el proceso serán referenciados por los nombres de sus cargos o nombres genéricos.

Misión

Todo Departamento de Tecnología tiene como misión de la gestión, coordinación y ejecución de proyectos en el ámbito de las tecnologías de información y comunicación, orientados al mejoramiento de la calidad académica y administrativa de la Universidad.

Funciones

El Departamento de Tecnología en general tiene las siguientes funciones:

- Proponer proyectos en el campo de las tecnologías de información y comunicación que procuren la calidad académica y administrativa de la Universidad, y establecer políticas universitarias de uso de las tecnologías de información y comunicación.
- Asesorar a los organismos de gobierno universitario en la implementación de sistemas de información y nuevas tecnologías en los procesos académicos, de investigación y de gestión.
- Incentivar, asesorar, coordinar y apoyar el uso de la informática en Facultades, Departamentos y demás unidades académicas, promover la cultura del cuidado, conservación, eficiencia y buen uso de los equipos y sistemas informáticos.
- Investigar e implementar nuevas tecnologías de información y comunicación que faciliten los procesos universitarios; planificar, evaluar y dar seguimiento a la implementación de sistemas informáticos integrales que permitan modernizar y agilitar los procesos académicos y administrativos.
- Diseñar, implementar y mantener los sistemas de información de la Universidad

empleando nuevas tecnologías de desarrollo de software.
- Implementar, administrar, mantener la red de datos y comunicación universitaria interna y externa.
- Responder por el buen funcionamiento de los servidores centrales, equipos de comunicaciones, almacenamiento, procesamiento y acceso a la información institucional.
- Administrar el centro de datos, desarrollar procesos de operación en coordinación con las unidades que usen este servicio y las demás que le confieran el Estatuto y los reglamentos de la Universidad. (Universidad, 2017)

2.2 Estructura del Departamento Tecnológico

Como la mayoría de Departamentos Tecnológicos el tomado para el análisis, está conformado por la siguiente estructura:

Coordinación de servicios informáticos: Brindar, promover, coordinar y evaluar los servicios de sistemas de información y comunicación, en las unidades administrativas, académicas y de investigación de la Universidad, procurando la mejora continua de estos servicios y su alineamiento con las necesidades de la comunidad universitaria.

Coordinación de sistemas de información: Dotar de sistemas de información innovadores y de calidad que automaticen los procesos y contribuyan a la consecución de los objetivos institucionales, y administrar los sistemas de información implementados.

Coordinación de redes y comunicaciones: Es la encargada de proporcionar una infraestructura tecnológica robusta y de la más alta calidad, y suministrar servicios de comunicaciones eficientes y eficaces que ayuden a satisfacer las necesidades informáticas institucionales.

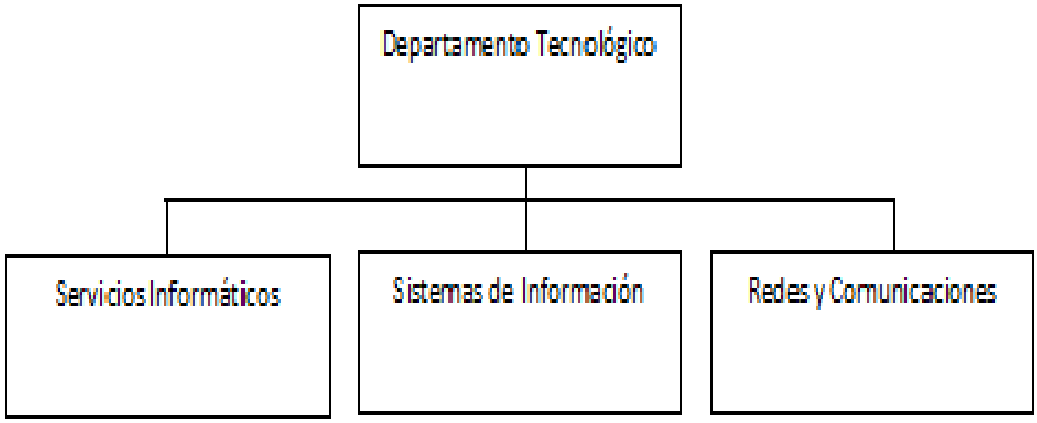


Figura 6. *Organigrama ejemplo del Departamento de Tecnología.*
Fuente: (Elaboración Propia) & (Universidad, 2017).

2.2.1 Recomendaciones sobre la estructura

Cada una de estas coordinaciones tienen su coordinador de área e ingenieros de primera y segunda línea. Siguiendo las recomendaciones de COBIT 5 para la gestión del riesgo es necesario tener una mejor organización de cargos y responsabilidades por lo que se recomienda un área de Seguridad Informática que ayude en la implementación y gestión tanto del plan de gestión de riesgos y éticos como del plan de contingencia. Para la asignación de los gestores se puede tomar ingenieros de segunda o primera línea de las tres coordinaciones, también es necesario conocer las responsabilidades de los cargos de gerencia que se involucran en la gestión de riesgos, por lo que se propone la siguiente matriz RACI para el Departamento Tecnológico y cargos que se involucran directamente con la gestión.

Tabla 6

Matriz RACI de cargos propuesto para el Departamento de Tecnología

	Cargos														
Actividades	Rector	Propietarios de los Procesos	Oficina de Gestión de Proyectos	Director de Riesgos (CRO)	Director de Seguridad de la Información	Comité de Riesgos Corporativos.	Auditoria	Director de Informática (CIO)	Coord. De Sistemas Información	Coord. Servicios Informáticos	Coord. Redes e Infraestructura	Gestor de Servicio	Gestor de Seguridad de la Información	Gestor de Continuidad del negocio	Gestor de Privacidad de la Información
Recopilar datos	I	R	R	R	R	I	C	A	R	R	R	R	R	R	R
Analizar el riesgo	I	R	C	R	C	I	R	A	C	C	C	C	C	C	C
Evaluar el riesgo	I	R	C	A	C	I	R	R	C	C	C	C	C	C	C
Comunicar el Riesgo	I	R	C	R	C	I	C	A	C	C	C	C	C	C	C
Tratar el Riesgo Tecnológico y ético	I	R	C	A	C	I	C	R	C	C	C	C	C	C	C
Responder al Riesgo	I	R	R	R	R	I	C	A	R	R	R	R	R	R	R

R: Responsable; A: Aprobador; C: Consultado; I: Informado
Fuente: (Elaboración Propia) & (Universidad, 2017) (ISACA, 2012).

2.3 Procesos

El Departamento de Tecnología está conformado por tres coordinaciones según lo revisado anteriormente. Para poder gestionar los riesgos es necesario conocer los procesos que tiene cada una de las áreas, estos procesos están documentados y asignados a responsables o gestores de los procesos. Las generaciones de los gráficos de los procesos son generadas en la

herramienta BIZAGE. Como Departamento Tecnológico se tienen clasificados los procesos en: transversales y propios de cada área, los mismos que se detallan a continuación.

2.3.1 Procesos Transversales

Entre los procesos transversales que realiza el departamento de tecnología están los siguientes:

Planificación estratégica de TI (Tecnologías de Información).

Gestión Financiera de T.I.

Capacitación al personal de T.I.

Gestión de la Comunicación.

Gestión de riesgos vea el grafico en el **Anexo C**.

Gestión de procesos.

Gestión de proyectos.

Gestión de la Disponibilidad.

Gestión de la Continuidad.

Gestión de eventos.

Gestión de problemas.

Gestión de la configuración.

2.3.2 Procesos de Servicios Informáticos

Entre la documentación recolectada están los siguientes procesos:

Capacitación a Usuarios Finales.

Mantenimiento preventivo y correctivo de equipos.

Gestión de Incidencias.

Informe técnico de equipo informático.

Gestión de requerimientos.

Voto electrónico.

Gestión de Accesos.

Reporte de Datos.

Gestión de Catálogo de Servicios.

Gestión de acuerdo de nivel de servicio.

2.3.3 Procesos de Sistemas de Información

La Coordinación de Sistemas de Información tiene los siguientes procesos levantados:

Gestión de Cambios de Sistemas de Información.

Pruebas de aceptación.

Despliegue Sistemas de Información.

Evaluación de Sistemas de Información.

Evaluación de respaldos.

2.3.4 Procesos de Redes y Comunicaciones

La Coordinación de Redes y Comunicaciones presenta los siguientes procesos:

Gestión de Usuarios.

Ampliación de red.

Configuración de equipos de comunicación.

Activación o actualización de extensión telefónica.

Creación de Servidores.

Respaldo de Servidores.

Recuperación de Información.

Hospedaje de Servidores Housing.

Publicación de dominio.

Instalación de servicios.

2.4 Evaluación de la Situación actual

Todo el estudio se centró en el Departamento de Tecnología, pero podría servir como marco de referencia para otros departamentos o direcciones de cualquier institución educativa.

La Figura 7 muestra los resultados obtenidos en las encuestas realizadas a las tres áreas del Departamento de Tecnología. Para la presente investigación se realizaron encuestas con varias preguntas, de acuerdo al área a la que pertenece el personal del departamento de tecnología, se determinó la situación actual en las tres áreas que lo conforman con respecto al conocimiento que se tiene sobre la existencia de un plan de gestión de riesgos, existencia de política de seguridad y existencia de un código de ética del departamento, se trabajó con una población o universo de 32 Ingenieros de Sistemas pertenecientes al Departamento de Tecnología, con un nivel de error del 5% y con un nivel de confianza de 95% obteniéndose la muestra de 30 Ingenieros para mayor detalle de los cálculos y de la fórmula utilizada para la obtención de la muestra referirse al **Anexo G**.

La muestra de 30 Ingenieros está dividida por coordinaciones:

Servicios Informáticos (7 profesionales).

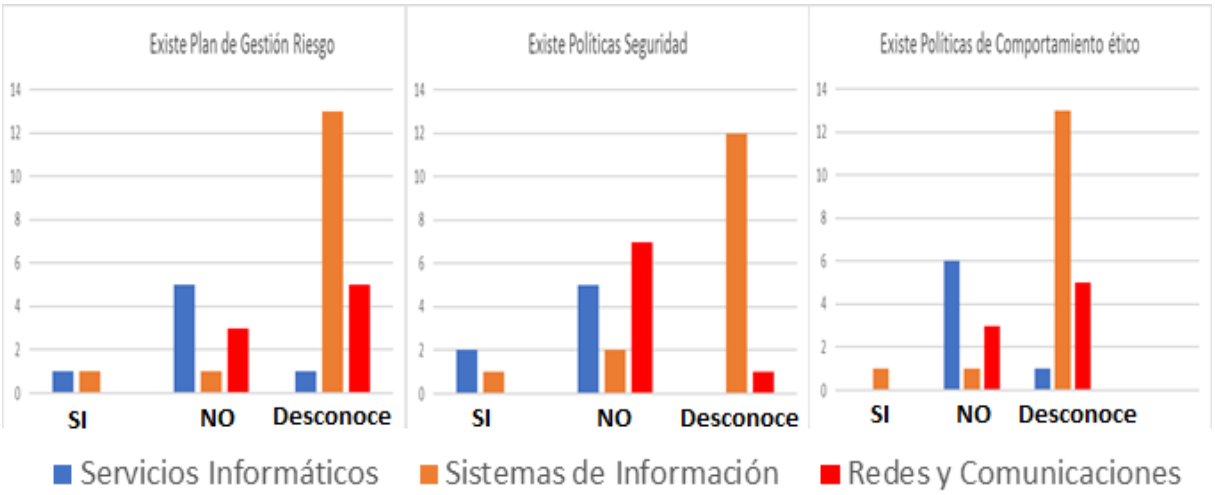
Sistemas de Información (15 profesionales).

Redes y comunicaciones (8 profesionales).

Obteniéndose los siguientes resultados. Para la realización de la encuesta se utilizó el formato del **Anexo A.**

Figura 7*. Resultados encuesta preguntas al Departamento de Tecnología por área.*
Datos obtenidos de las tres áreas del Departamento de Tecnología. Fuente: (Elaboración Propia).

La primera pregunta hace referencia a si existe un plan de gestión de riesgos tecnologicos.



Se puede apreciar que la mayoria del personal del Departamento de tecnología manifiesta que desconoce o que no existe un plan de gestión de riesgos tecnológicos en su lugar de trabajo. Los pocos que manifiestan que si existe señalaron los siguientes planes de gestión de acuerdo a su área:

Servicios Informáticos: Respaldo eléctrico y de datos, seguridad contra incendios en el Data Center.

Sistemas de Información: Respaldos de todo el servidor de desarrollo, producción, etc.

Redes y comunicaciones: No existe documentado pero la responsabilidad del puesto exige que tengan procedimientos de recuperación de desastres.

Por lo que se pudo determinar con la información solicitada al Departamento de Tecnología, que no existe un Plan de Gestión de Riesgos Tecnológicos.

Con respecto a la segunda pregunta, ¿existen políticas de seguridad? se puede apreciar que la gran mayoría manifiesta que desconoce o no existen políticas de seguridad informática. Los pocos que manifiestan conocer de la existencia de políticas redactaron las siguientes:

Servicios Informáticos: Gestión de claves de usuario para sistemas y servidores, antivirus, firewall, niveles y privilegios de acceso a sistemas y equipos.

Sistemas de Información: Acceso a servidores mediante clave pública.

Redes y Comunicaciones: Manifiestan que no tienen formalmente, pero trabajan en base a estándares.

De acuerdo a la investigación en la institución, se encontró que en el 2014 se aprobaron políticas del Departamento de Tecnología. De esta forma se determinó que existe una falta de difusión y socialización con el personal técnico, lo cual se evidencia con los resultados de la encuesta.

La tercera y última pregunta hace referencia a si existe un plan de comportamiento ético en su área de trabajo, la gran mayoría desconoce, pero los pocos que manifiestan que si conocen de políticas de comportamiento ético comentan lo siguiente:

Sistemas de Información: Cumplir horarios y transmitir conocimientos.

Redes y Comunicación: El reglamento interno del personal los contempla, pero no hay una difusión, aunque el desconocimiento no exime de responsabilidad.

El Consejo Universitario de la Institución, con fecha 15 de mayo del 2012 aprobó en sesión ordinaria el Código de ética institucional, que se aplica de forma general para toda la institución.

Igualmente, que en la pregunta 2, se evidencia que el problema es la falta de difusión de las normativas y políticas.

De esta forma se sugiere que el código de ética de la institución podría contener ciertas normas de comportamiento ético ligado al plan de gestión de riesgos asumiendo responsabilidades propias del personal que labora en el Departamento de Tecnología que ayuden en el tratamiento eficaz y oportuno del riesgo.

Capítulo 3

Desarrollo de la propuesta del plan de Gestión de Riesgos de Tecnologías de Información y gestión ética para el Departamento de Tecnología

3.1 Proceso propuesto

La propuesta del plan de Gestión de Riesgos de Tecnología de información y de gestión ética para el departamento de tecnología ha sido elaborado basándose en el estudio en una Institución educativa del sector público, obteniéndose resultados satisfactorios, lo cual va a permitir su mejora interna y externa en el tratamiento de los riesgos, para tomarlo como referencia en la implementación en otros departamentos u organizaciones del sector.

El proceso se definió siguiendo los lineamientos de los estándares descritos en el capítulo 1, utilizando la metodología de MAGERIT y para el plan gestión ética utilizando la norma ISO 26000.

3.2 Establecimiento del Contexto

El plan de gestión de riesgos se realiza en el marco de la norma ISO 31000:2011, por tal motivo se debe utilizar la lista de activos propuesta por MAGERIT para tener estandarizado los nombres de los mismos. Para la investigación se identificaron los activos por cada área que conforma el Departamento de Tecnología y que en base a encuestas y la utilización de la herramienta PILAR (PILAR, 2017) se pudo determinar que por su impacto puede interferir con la misión y objetivos del Departamento de Tecnología dentro de la institución. Luego de la identificación de los activos se debe valorar el riesgo de forma cualitativa determinando su impacto y probabilidad de ocurrencia y así poder determinar las acciones o salvaguardas para poder mitigar el riesgo. Para conocer de mejor forma el contexto organizacional interno y

externo se utiliza la matriz FODA de forma general para cualquier Departamento de Tecnología.

Tabla 7

Ejemplo de FODA del Departamento de Tecnología

Fortalezas	**Debilidades**
• Apoyo de la Gerencia para la generación de ideas y oportunidades de mejora. • Líderes de área en coordinación permanente con objetivos claros de lo que persigue la institución. • Personal comprometido con capacidad técnica y experiencia profesional. • Plan de capacitación de acuerdo a las necesidades del personal	• Falta de incorporación de buenas prácticas y estándares. • Débil gestión en los procesos, falta de políticas, procedimientos, estándares de gestión y evaluación de servicio. • Limitado espacio físico en infraestructura.
Oportunidades	**Amenazas**
• Políticas de estado que apoyan a las instituciones de Educación superior para alcanzar la excelencia académica • Iniciativa Gubernamental del Plan Nacional de Gobierno electrónico • Desarrollos de nuevas tecnologías y buenas prácticas de gestión enfocadas en los sistemas educativos. • Capacidad de adaptación a las herramientas tecnológicas para generar soluciones a bajo costo.	• Cambios inesperados en las competencias y estructura de la organización • Procedimientos administrativos burocráticos en las adquisiciones. • Resistencia al cambio, falta de disposición y compromiso de las distintas unidades. • Limitaciones gubernamentales en la asignación de recursos económicos.

Fuente: (Universidad, 2017) & (Elaboración propia).

3.3 Identificación del riesgo

Utilizando la tabla de elementos propuesta por MAGERIT y utilizando la herramienta PILAR y los datos de las encuestas se procede a categorizar e identificar los activos.

Figura 8. *Categorización de Activos con la herramienta PILAR.*
Fuente: (PILAR, 2017)

En la Figura 8 se demuestra que al utilizar la herramienta PILAR y de las encuestas realizadas al personal técnico facilita la clasificación de los activos. Posteriormente, se va a utilizar la matriz de riesgos para analizar los riesgos que generen mayor impacto a la organización y se van a seleccionar tres activos por área responsable para realizar los demás pasos de la metodología del Plan de Gestión de riesgos En la Tabla 6, se citan los activos identificados en base al análisis de procesos, encuestas al personal del Departamento

Tecnológico y la lista de elementos que nos da MAGERIT para la estandarización de los nombres de los activos.

Tabla 8
Clasificación de los Activos

Activos	Categorías	Área Responsable
a) Datos de Carácter Personal	Activos esenciales	Servicios Informáticos
b) Datos Institucionales	Activos esenciales	Servicios Informáticos
c) Copias de Respaldo	Activos esenciales	Redes y Comunicaciones
d) Código Fuente	Activos esenciales	Sistemas de Información
e) Word Wide Web	Servicios Internos	Redes y Comunicaciones
f) Aplicaciones de Desarrollo Propio	Aplicaciones	Sistemas de Información
g) Servidor de Aplicaciones	Aplicaciones	Sistemas de Información
h) Ofimática	Aplicaciones	Servicios Informáticos
i) Antivirus	Aplicaciones	Servicios Informáticos
j) Sistema de Gestión de Base de Datos	Aplicaciones	Sistemas de Información
k) Informática Personal	Equipos	Servicios Informáticos
l) Servidores	Equipos	Redes y Comunicaciones
m) Red Local	Comunicaciones	Redes y Comunicaciones
n) Red Inalámbrica	Comunicaciones	Redes y Comunicaciones
o) Internet	Comunicaciones	Redes y Comunicaciones
p) Red Telefónica	Comunicaciones	Redes y Comunicaciones
q) Equipos de Climatización	Elementos auxiliares	Redes y Comunicaciones

r) Correo electrónico	Servicios subcontratados	Redes y Comunicaciones
s) Servicio Internet Proveedor	Servicios subcontratados	Redes y Comunicaciones
t) Generadores eléctricos	Servicios subcontratados	Redes y Comunicaciones
u) Data Center	Instalaciones	Redes y Comunicaciones
v) Voto electrónico	Servicios Internos	Sistemas de Información
w) Usuarios Internos	Personal	Universidad
x) Usuarios externos	Personal	Ciudad
y) Operadores	Personal	Universidad
z) Proveedores	Personal	Ciudad

Nota: Datos obtenidos de las encuestas y estandarizados con la tabla de elementos de MAGERIT, ordenados por categorías.
Fuente: (Elaboración Propia).

3.4 Matriz del riesgo

La matriz de riesgos muestra gráficamente la evaluación del riesgo de forma cualitativa, utilizando dos aspectos: impacto y probabilidad del mismo. Se adaptó la matriz presentada por COBIT 5 con las amenazas de la metodología MAGERIT. Una vez identificados los activos se procede al análisis de las amenazas que provocan estas fallas, para esto se necesita la información obtenida de las coordinaciones del Departamento de Tecnología.

El valor del riesgo (R) se obtiene de la multiplicación del impacto (I) por la probabilidad (P). Se relacionará el nivel del riesgo por rangos y colores: riesgo bajo rango de 1-5 color verde, riesgo medio rango de 6-10 color amarillo y riesgo alto rango de 11-15 color rojo.

$$R= (I * P)$$

Por impacto se debe comprender como las consecuencias o efectos que se presentarían en la organización si el riesgo se materializa. El impacto podrá ser clasificado como:

- 1 leve
- 2 bajo

- 3 medio
- 4 alto y
- 5 extremo

Por otro lado, la probabilidad es la posibilidad subjetiva u objetiva de que el riesgo se llegue a materializar esto dependerá del tipo de amenaza que puede ser de origen natural, entorno, defectos o fallos y por negligencia humana. La probabilidad podrá ser clasificado como:

1 poco probable,

2 medio probable y

3 muy probable.

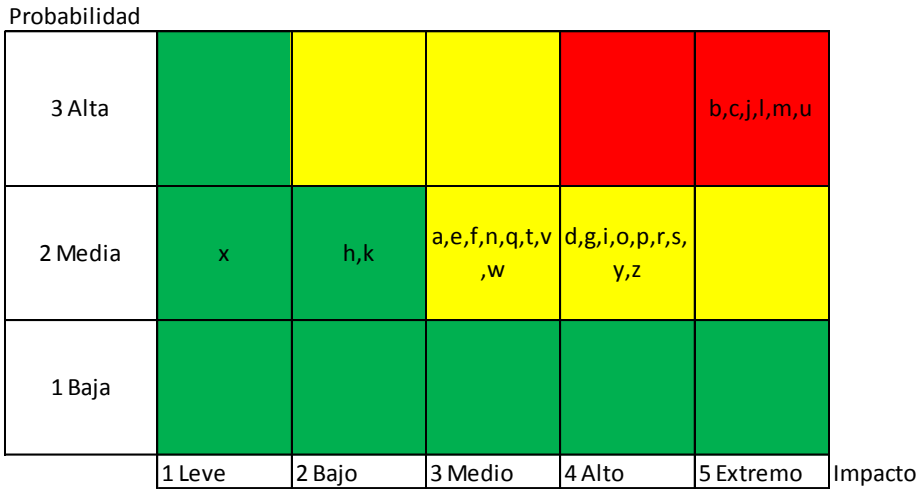


Figura 9. *Matriz del riesgo.*
Fuente: (Elaboración Propia) & (ISACA, 2012)

Esta matriz de riesgos fue el resultado de los cálculos realizados en la Tabla 7. Para obtener los resultados del riesgo promedio de cada activo se calificó el impacto desde el nivel 1 leve a 5 extremo el impacto es la consecuencia en el caso de que el riesgo se materialice y no poder disponer del activo en la organización y la probabilidad en base a las amenazas que se puede tener calificadas desde 1 probabilidad baja hasta 3 probabilidad alta con esto se obtiene un

promedio de riesgo por amenaza. Para obtener el riesgo es la multiplicación del impacto por la probabilidad y al final se obtuvo el promedio de todos los riesgos parciales para poder determinar cuáles son los activos con mayor vulnerabilidad y que impactarían desfavorablemente a la organización.

Tabla 9
Calculo de los riesgos promedios por Activo.

Activos	Impacto	Probabilidad Riesgo									
		Naturaleza			Entorno			Defectos o Daños de Aplicaciones		Negligencia Personal Deliberada o Accidental	Riesgo Promedio
		Fuego (2)	Agua (1)	Rayos (2)	Ataques Hackers (2)	Robo (1)	Virus (3)	Software (2)	Hardware (3)	Mal Uso, Respaldos, Accesos Información (3)	Suma Riesgos /9
a) Datos de Carácter Personal	3	6	3	6	6	3	9	6	9	9	6
b) Datos Institucionales	5	10	5	10	10	5	15	10	15	15	11
c) Copias de Respaldo	5	10	5	10	10	5	15	10	15	15	11
d) Código Fuente	4	8	4	8	8	4	12	8	12	12	8
e) Word Wide Web	3	6	3	6	6	3	9	6	9	9	6
f) Aplicaciones de Desarrollo Propio	3	6	3	6	6	3	9	6	9	9	6
g) Servidor de Aplicaciones	4	8	4	8	8	4	12	8	12	12	8
h) Ofimática	2	4	2	4	4	2	6	4	6	6	4

i) Antivirus	4	8	4	8	8	4	12	8	12	12	8
j) Sistema de Gestión de Base de Datos	5	10	5	10	10	5	15	10	15	15	11
k) Informática Personal	2	4	2	4	4	2	6	4	6	6	4
l) Servidores	5	10	5	10	10	5	15	10	15	15	11
m) Red Local	5	10	5	10	10	5	15	10	15	15	11
n) Red Inalámbrica	3	6	3	6	6	3	9	6	9	9	6
o) Internet	4	8	4	8	8	4	12	8	12	12	8
p) Red Telefónica	4	8	4	8	8	4	12	8	12	12	8
q) Equipos de Climatización	3	6	3	6	6	3	9	6	9	9	6
r) Correo electrónico	4	8	4	8	8	4	12	8	12	12	8
s) Servicio Internet Proveedor	4	8	4	8	8	4	12	8	12	12	8
t) Generadores eléctricos	3	6	3	6	6	3	9	6	9	9	6
u) Data Center	5	10	5	10	10	5	15	10	15	15	11

v) Voto electrónico	3	6	3	6	6	3	9	6	9	9	6
w) Usuarios Internos	3	6	3	6	6	3	9	6	9	9	6
x) Usuarios externos	1	2	1	2	2	1	3	2	3	3	2
y) Operadores	4	8	4	8	8	4	12	8	12	12	8
z) Proveedores	4	8	4	8	8	4	12	8	12	12	8

Riesgo = Impacto x Probabilidad.
Fuentes: (Elaboración Propia) & (ISACA, 2012)

Con la matriz de riesgos se puede determinar que activos son de mayor vulnerabilidad se seleccionaron tres por área y un activo que tiene un riesgo bajo para poder utilizarlos como ejemplo en la metodología de MAGERIT. Como se muestra en la siguiente Figura.

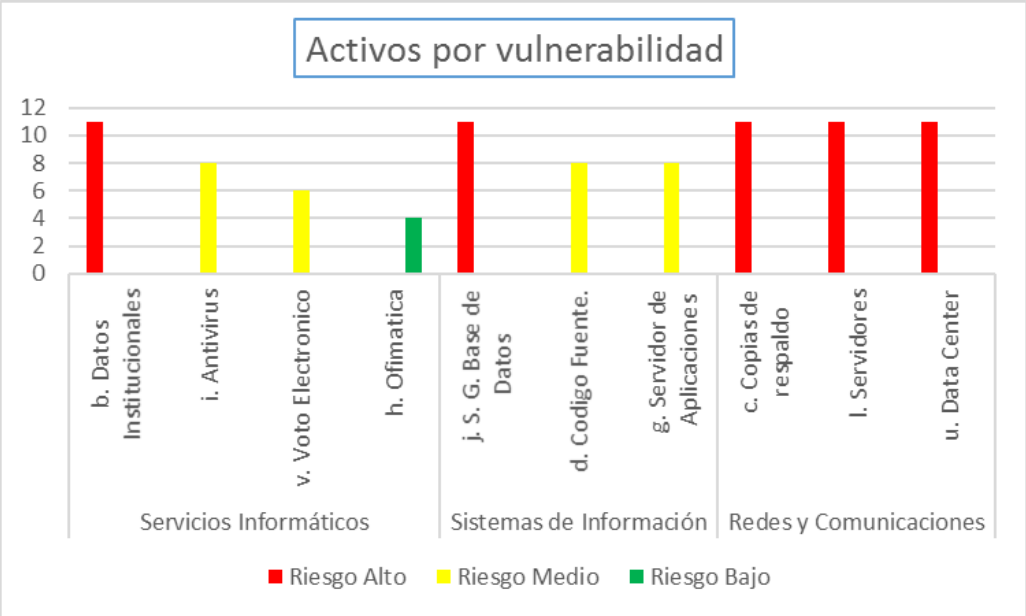


Figura 10. *Activos por vulnerabilidad y por área.*
Fuente: (Elaboración Propia).

3.5 Análisis del riesgo

En esta etapa se analiza el activo con respecto a su disponibilidad, integridad y confidencialidad. Cada una de esta tendrá un valor de acuerdo a la escala propuesta por MAGERIT y representada en la Tabla 8.

Disponibilidad (D): Nos debemos preguntar que perjuicio tendríamos al no poderlo utilizar el activo.

Integridad (I): Nos debemos preguntar que perjuicio se tendría al estar dañado o corrupto el activo.

Confidencialidad (C): Nos debemos preguntar que daño causaría que lo conociera el que no debe. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Tabla 10
Valor de Criterio

Valor	***Criterio***
10	*Daño Extremo*
9	*Daño Muy Alto*
6 al 8	*Daño Alto*
3 al 5	*Daño Medio*
1 al 2	*Daño Bajo*
0	*Daño Despreciable*

Valor de Criterio de daño recomendado por MAGERIT.
Fuentes: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

3. 6 Evaluación del riesgo

Autenticidad (A): Nos debemos preguntar qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa. (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar)

Trazabilidad del uso del servicio (T): ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?

Trazabilidad del acceso a los datos: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

Valoración (V): es la determinación del coste que supondría recuperarse de una incidencia que destrozara el activo. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

[uni001] análisis de riesgos > activos > valoración de los activos

Editar Exportar Importar

activo	[D]	[I]	[C]	[A]	[T]	[V]
ACTIVOS						
[B] Activos esenciales						
[backup] Copias de respaldo	[9]	[8]	[7]	[9]	[7]	[8]
[dinst] Datos Institucionales	[9]	[8]	[9]	[9]	[7]	[8]
[source] Codigo Fuente	[6]	[7]	[7]	[8]	[6]	[7]
[E] Equipamiento						
[SW] Aplicaciones						
[dbms] Sistema de gestión de Base de Datos	[9]	[9]	[8]	[8]	[9]	[7]
[av] Antivirus	[5]	[5]	[5]	[7]	[6]	[6]
[office] Ofimática	[2]	[2]	[2]	[1]	[2]	[3]
[app] Servidor de Aplicaciones	[6]	[7]	[8]	[7]	[8]	[6]
[HW] Equipos						
[host] Servidores	[9]	[8]	[8]	[8]	[7]	[8]
[IS] Servicios internos						
[ve] Voto electrónico	[5]	[5]	[8]	[8]	[5]	[6]
[L] Instalaciones						
[dc] Data Center	[9]	[8]	[8]	[9]	[7]	[9]

Figura 11. *Valoración de los activos.*
Fuente: (Elaboración Propia) & (PILAR, 2017)

En las Tablas 9 y 10 se realiza la identificación y valoración de las amenazas de acuerdo a su origen propuestas por MAGERI (2012) estas pueden ser:

[N] Desastres Naturales.

[I] de Origen Industrial.

[E] Errores y Fallos No Intencionados.

[A] Ataques Deliberados.

La valoración de las amenazas está dada por su degradación y probabilidad. Los activos pueden tener varias amenazas. Debido a que es una valoración cualitativa no se considerará en el análisis del campo (V) valor. De acuerdo al activo la herramienta PILAR y la opinión de los expertos sugieren una serie de posibles amenazas. **Anexo B.**

Tabla 11
Degradación y Probabilidad

Degradación o Impacto del Valor					Probabilidad o Frecuencia de Ocurrencia			
MA	100	muy alta	facil		MA	100	muy frecuente	a diario
A	10	alta	medio		A	10	frecuente	mensualmente
M	1	media	difícil		M	1	normal	una vez al año
B	1/10	baja	muy dificil		B	1/10	poco frecuente	cada varios años
MB	1/100	muy baja	extremadamente dificil		MB	1/100	muy poco frecuente	siglos

Fuentes: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Tabla 12
Valoración de las amenazas

[B] Activos Esenciales								
Activo	**Código**	**Amenaza**	**F**	**D**	**I**	**C**	**A**	**T**
[backup] Copias de Respaldo	E.15	Alteración de la Información	1		1%			
	E.18	Destrucción dela Información	1	1%				
	E.19	Fugas de Información	1			10%		
	A.5	Suplantación de Identidad	10		10%	50%	100%	
	A.6	Abuso de privilegios de Acceso	10	1%	10%	50%		
	A.11	Acceso no autorizado	100		10%	50%		
[dins] Datos Institucionales	E.15	Alteración de la Información	1		1%			
	E.18	Destrucción de la Información	1	1%				
	E.19	Fugas de Información	1			10%		
	A.5	Suplantación de Identidad	10		10%	50%	100%	
	A.6	Abuso de privilegios de Acceso	10	1%	10%	50%		
	A.11	Acceso no autorizado	100		10%	50%		
[source] Código Fuente	E.15	Alteración de la Información	1		1%			
	E.18	Destrucción de la Información	1	1%				
	E.19	Fugas de Información	1			10%		
	A.5	Suplantación de Identidad	10		10%	50%	100%	
	A.6	Abuso de privilegios de Acceso	10	1%	10%	50%		
	A.11	Acceso no autorizado	100		10%	50%		
[E] Equipamiento								

Activo	Código	Amenaza	F	D	I	C	A	T
[SW] Aplicación [dbms]+B41 Sistema de Gestión de Base de Datos	I.5	Avería de origen físico o lógico	1	50%				
	E.8	Difusión de software dañino	1	10%	10%	10%		
	E.20	Vulnerabilidades de los programas	1	1%	20%	20%		
	E.21	Errores de Mantenimiento/actualización de programa	10	1%	1%			
	A.8	Difusión de software dañino	1	100%	100%	100%		
	A.22	Manipulación de programas	1	50%	100%	100%		
[SW] Aplicación [av] Antivirus	I.5	Avería de origen físico o lógico	1	50%				
	E.8	Difusión de software dañino	1	10%	10%	10%		
	E.20	Vulnerabilidades de los programas	1	1%	20%	20%		
	E.21	Errores de Mantenimiento/actualización de programa	10	1%	1%			
	A.8	Difusión de software dañino	1	100%	100%	100%		
	A.22	Manipulación de programas	1	50%	100%	100%		
[SW] Aplicación [office] Ofimática	I.5	Avería de origen físico o lógico	1	50%				
	E.8	Difusión de software dañino	1	10%	10%	10%		
	E.20	Vulnerabilidades de los programas	1	1%	20%	20%		
	E.21	Errores de Mantenimiento/actualización de programa	10	1%	1%			
	A.8	Difusión de software dañino	1	100%	100%	100%		
	A.22	Manipulación de programas	1	50%	100%	100%		
[SW] Aplicación [app] Servidor de Aplicaciones	I.5	Avería de origen físico o lógico	1	50%				
	E.8	Difusión de software dañino	1	10%	10%	10%		
	E.20	Vulnerabilidades de los programas	1	1%	20%	20%		
	E.21	Errores de Mantenimiento/actualización de programa	10	1%	1%			
	A.8	Difusión de software dañino	1	100%	100%	100%		
	A.22	Manipulación de programas	1	50%	100%	100%		

[HW] Equipos [host] Servidores	N.1	Fuego	0,2	100%				
	N.2	Daños por agua	0,2	50%				
	N.*	Desastres naturales	0,2	100%				
	I.1	Fuego	0,5	100%				
	I.2	Daños por agua	0,5	50%				
	I.*	Desastres industriales	0,5	100%				
	I.3	Contaminación medioambiental	0,1	50%				
	I.4	Contaminación electromagnética	1	10%				
	I.5	Avería de origen físico o lógico	1	50%				
	I.6	Corte de suministro eléctrico	1	100%				
	I.7	Condiciones inadecuadas de temperatura o humedad	1	100%				
	I.11	Emanaciones electromagnéticas	1			1%		
	E.23	Errores de Mantenimiento/actualización de equipos	1	15%				
	E.24	Caída de sistema por agotamiento de recursos	11	50%				
	E.25	Pérdida de equipos	0,1	100%		100%		
	A.7	Uso No previsto	1	1%	1%	10%		
	A.11	Acceso No autorizado	1	10%	10%	50%		
	A.23	Manipulación del Hardware	0,5	50%		50%		
	A.24	Denegación de Servicio	2	100%				
	A.25	Robo de Equipos	0,1	100%		100%		
	A.26	Ataque Destructivo	1	100%				
[IS] Servicio Interno								
Activo	**Código**	**Amenaza**	**F**	**D**	**I**	**C**	**A**	**T**
[ve] Voto Electrónico	E.1	Errores de los usuarios	1	15%	15%	15%		
	E.2	Errores del Administrador del Sistema	1	25%	25%	25%		
	E.15	Alteración de la Información	1		1%			
	E.18	Destrucción de la Información	1	10%				
	E.19	Fugas de Información	1			10%		
	E.24	Caída de sistema por agotamiento de recursos	10	50%				
	A.5	Suplantación de Identidad	1.1		50%	50%	100%	

	A.6	Abuso de privilegios de Acceso	1.1	1%	10%	10%	100%	
	A.7	Uso no previsto	1.1	1%	10%	10%		
	A.11	Acceso no autorizado	1.1		10%	50%	100%	
	A.13	Repudio (negación de actuación)	5.5					100%
	A.15	Modificación de la Información	11		50%			
	A.18	Destrucción de la Información	1.1	50%				
	A.24	Denegación de servicio	11	50%				
[L] Instalaciones								
Activo	**Código**	**Amenaza**	**F**	**D**	**I**	**C**	**A**	**T**
[dc] Data Center	N.1	Fuego	1	100%				
	N.2	Daños por agua	1	100%				
	N.*	Desastres naturales	0,5	100%				
	I.1	Fuego	1	100%				
	I.2	Daños por agua	1	100%				
	I.*	Desastres industriales	1	100%				
	I.3	Contaminación medioambiental	1	10%				
	I.4	Contaminación electromagnética	0,1	10%				
	I.6	Corte de suministro eléctrico	1	10%				
	I.9	Interrupción de otros servicios	1	10%				
	I.11	Emanaciones electromagnéticas	1			1%		
	E.23	Errores de Mantenimiento/actualización de equipos	1	10%				
	A.6	Abuso de privilegios de Acceso	1	10%				
	A.7	Uso no previsto	1	10%				
	A.11	Acceso no autorizado	1		10%	50%		
	A.23	Manipulación del hardware	1	50%		50%		
	A.25	Robo de equipos	0,8	100%				
	A.26	Ataque destructivo	0,1	100%				
	A.27	Ocupación enemiga	1	100%				

Nota: Las amenazas marcadas con rojo tienen mayor probabilidad de materializarse
Fuente: (Elaboración Propia) & (PILAR, 2017)

3.7 Tratamiento del riesgo

En la investigación se pudo determinar que para el tratamiento del riesgo y como poder mitigarlo se utiliza lo que MAGERIT denomina salvaguardas. Una salvaguarda es eficaz cuando su factor llega al 100% de eficacia contra el riesgo. La salvaguarda se aplica de acuerdo al impacto y probabilidad de la amenaza. PILAR da una lista de salvaguardas que se pueden aplicar o el personal del departamento también puede incluir su salvaguarda.

Según MAGERIT (2012) propone estas escalas para el Nivel de Madurez:

- L0: no existe
- L1: inicializado
- L2: reproducible e intuitivo;
- L3: proceso definido
- L4: Gestionado y Medible
- L5: Optimizado.

Para la elaboración de las responsabilidades éticas es necesario tomar los lineamientos que se detallan en el **Anexo H.**

Tabla 13
Valoración de las Salvaguardas y Responsabilidades éticas.

Activos	Código Amenaza	Salvaguardas	Factor	Responsabilidades éticas	Área Responsable	Tiempo Respuesta	Nivel Actual	Nivel Optimo
[backup] Copias de Respaldo; [dins] Datos Institucionales; [source] Código Fuente	E.15	Protección de la Información	60%	Encriptar datos importantes. Datos en la nube.	Redes y Servicios	Inmediato	L2	L4
	E.18	Copias de Seguridad de los datos	80%	Restituir el backup.	Redes e Infraestructura	Corto plazo	L3	L4
	E.19	Identificación y autentificación	80%	Personal evitar divulgar o robar contraseñas.	Redes e Infraestructura	Inmediato	L3	L5
	A.5	Control de acceso lógico	70%	Evitar plagios o falsificar los accesos. Evitar alterar información en la bases de datos	Redes e Infraestructura	Corto plazo	L2	L4
	A.6	Uso de firmas electrónicas	80%	La firma electrónica es personal e intransferible	Servicios Informáticos	Inmediato	L3	L5
	A.11	Accesos con huella	60%	No permitir el ingreso de desconocidos	Redes e Infraestructura	Inmediato	L3	L5
Activos	**Código Amenaza**	**Salvaguardas**	**Factor**	**Responsabilidades éticas**	**Área Responsable**	**Tiempo Respuesta**	**Nivel Actual**	**Nivel Optimo**
[dbms] Sistema de Gestión de Base de Datos; [av] Antivirus; [office] Ofimática; [app] Servidor de Aplicacione	I.5	Protección de los equipos informáticos	60%	Conectar correctamente los UPS, Revisiones eléctricas.	Servicios Informáticos	Corto plazo	L2	L4
	E.8	Herramientas de Seguridad.	70%	Ejecutar el antivirus; Levantar los Firewall. No abrir correos maliciosos	Redes e Infraestructura y Servicios Informáticos	Inmediato	L3	L4

s;	E.20	Perfiles de Seguridad	60%	Configurar perfiles de seguridad en el dominio parches y antivirus.	Redes e Infraestructura y Servicios Informáticos	Corto plazo	L2	L4
	E.21	Cambios Actualizaciones y mantenimientos	50%	Personal ejecutar parches de los programas.	Sistemas de Información y Servicios Informáticos	Corto plazo	L2	L4
	A.8	Herramientas de Seguridad.	70%	Ejecutar el antivirus; Levantar los Firewall. No abrir correos maliciosos	Redes e Infraestructura y Servicios Informáticos	Inmediato	L3	L4
	A.22	Perfil de aplicaciones de prueba	50%	No permitir la manipulación de programas en producción	Sistemas de Información y Servicios Informáticos	Inmediato	L3	L5
[host] Servidores	N.1	Protección de los equipos informáticos	60%	Utilizar extintores para equipo informático	Servicios Informáticos y Redes e Infraestructura	Inmediato	L4	L4
	N.2	Protección de los equipos informáticos	60%	Evitar el paso de tuberías de agua cerca de equipos	Redes e Infraestructura y Servicios Informáticos	Corto plazo	L4	L4
	N.*	Protección de los equipos informáticos	50%	Poseer equipos de Backup	Redes e Infraestructura y Servicios Informáticos	Corto plazo	L3	L4
	I.1	Protección de los equipos informáticos	60%	Utilizar extintores para equipo informático	Servicios Informáticos y Redes e Infraestructura	Inmediato	L4	L4

	I.2	Protección de los equipos informáticos	60%	Evitar el paso de tuberías de agua cerca de equipos	Redes e Infraestructura y Servicios Informáticos	Corto plazo	L4	L4
	I.*	Protección de los equipos informáticos	50%	Poseer equipos de Backup	Redes e Infraestructura y Servicios Informáticos	Corto plazo	L3	L4
	I.3	Climatización	50%	Poseer salas herméticas	Redes e Infraestructura y Servicios Informáticos	Largo plazo	L2	L3
	I.4	Climatización	50%	Poseer salas herméticas	Redes e Infraestructura y Servicios Informáticos	Largo plazo	L2	L3
	I.5	Aseguramiento de la disponibilidad	70%	Poseer equipos de Backup	Servicios Informáticos	Corto plazo	L3	L4
	I.6	Suministro eléctrico	80%	Tener previsto Generadores eléctricos y UPS	Redes e Infraestructura y Servicios Informáticos	Inmediato	L4	L4
	I.7	Climatización	50%	Poseer salas herméticas con control de temperatura	Redes e Infraestructura y Servicios Informáticos	Corto plazo	L2	L3
	I.11	Climatización	50%	Poseer salas herméticas	Redes e Infraestructura y Servicios Informáticos	Largo plazo	L2	L3

	E.23	Protección de los equipos informáticos	50%	Poseer equipos de Backup	Redes e Infraestructura y Servicios Informáticos	Corto plazo	L3	L4
	E.24	Renovación de equipos	70%	Renovar equipos que pasaron su vida útil	Servicios Informáticos	Corto plazo	L3	L4
	E.25	Protección de los equipos informáticos	50%	Poseer un seguro contra perdidas de equipos	Todos	Corto plazo	L3	L4
	A.7	Perfiles de Seguridad	60%	Usuarios invitados con restricción de perfil	Todos	Inmediato	L3	L4
	A.11	Identificación y autentificación	80%	Personal evitar divulgar o robar contraseñas.	Redes e Infraestructura	Inmediato	L3	L5
	A.23	prevención de intrusión	70%	Utilizar herramientas de prevención de intrusos en el equipo; no divulgar contraseñas	Todos	Corto plazo	L2	L4
	A.24	Control de acceso lógico	70%	Evitar plagios o falsificar los accesos.	Redes e Infraestructura	Corto plazo	L2	L4
	A.25	Control de acceso físico	60%	Evitar el ingreso a personas desconocidas; Poseer un seguro; Cámaras de vigilancia	Todos	Corto plazo	L3	L4
	A.26	Protección de las Instalaciones	50%	Poseer Data Center de emergencia	Redes e Infraestructura	Largo plazo	L2	L4
[ve] Voto Electrónico	E.1	Capacitación a los usuarios	70%	Poseer manuales y capacitar	Servicios Informáticos	Inmediato	L3	L4

	E.2	Capacitación al administrador	70%	Poseer manuales y capacitar. Poner atención en las actividades.	Servicios Informáticos	Inmediato	L3	L4
	E.15	Protección de la Información	60%	Encriptar datos importantes. Datos en la nube.	Redes y Servicios	Inmediato	L2	L4
	E.18	Copias de Seguridad de los datos	80%	Restituir el backup.	Redes e Infraestructura	Corto plazo	L3	L4
	E.19	Identificación y autentificación	80%	Personal evitar divulgar o robar contraseñas.	Redes e Infraestructura	Inmediato	L3	L5
	E.24	Renovación de equipos	70%	Renovar equipos que pasaron su vida útil	Servicios Informáticos	Corto plazo	L3	L4
	A.5	Control de acceso lógico	70%	Evitar plagios o falsificar los accesos.	Redes e Infraestructura	Corto plazo	L2	L4
	A.6	Uso de firmas electrónicas	80%	La firma electrónica es personal e intransferible	Servicios Informáticos	Inmediato	L3	L5
	A.7	Perfiles de Seguridad	60%	Usuarios invitados con restricción de perfil	Todos	Inmediato	L3	L4
	A.11	Identificación y autentificación	80%	Personal evitar divulgar o robar contraseñas.	Redes e Infraestructura	Inmediato	L3	L5
	A.13	Formación y concienciación	70%	Formar en valores para que cambie su actitud	Servicios Informáticos	Inmediato	L2	L4
	A.15	Protección criptográfica	70%	Tener los resultados del voto encriptados	Servicios Informáticos	Inmediato	L4	L4
	A.18	Copias de Seguridad de los datos	80%	Restituir el backup.	Redes e Infraestructura	Corto plazo	L3	L4

	A.24	Control de acceso lógico	70%	Evitar plagios o falsificar los accesos.	Redes e Infraestructura	Corto plazo	L2	L4
Activos	**Código Amenaza**	**Salvaguardas**	**Factor**	**Responsabilidades éticas**	**Área Responsable**	**Tiempo Respuesta**	**Nivel Actual**	**Nivel Optimo**
[dc] Data Center	N.1	Protección de los equipos informáticos	60%	Utilizar extintores para equipo informático	Servicios Informáticos y Redes e Infraestructura	Inmediato	L4	L4
	N.2	Protección de los equipos informáticos	60%	Evitar el paso de tuberías de agua cerca de equipos	Redes e Infraestructura y Servicios Informáticos	Corto plazo	L4	L4
	N.*	Protección de los equipos informáticos	50%	Poseer equipos de Backup	Redes e Infraestructura y Servicios Informáticos	Corto plazo	L3	L4
	I.1	Protección de los equipos informáticos	60%	Utilizar extintores para equipo informático	Servicios Informáticos y Redes e Infraestructura	Inmediato	L4	L4
	I.2	Protección de los equipos informáticos	60%	Evitar el paso de tuberías de agua cerca de equipos	Redes e Infraestructura y Servicios Informáticos	Corto plazo	L4	L4
	I.*	Protección de los equipos informáticos	50%	Poseer equipos de Backup	Redes e Infraestructura y Servicios Informáticos	Corto plazo	L3	L4
	I.3	Climatización	50%	Poseer salas herméticas	Redes e Infraestructura y Servicios Informáticos	Largo plazo	L2	L3

	I.4	Climatización	50%	Poseer salas herméticas	Redes e Infraestructura y Servicios Informáticos	Largo plazo	L2	L3
	I.6	Suministro eléctrico	80%	Tener previsto Generadores eléctricos y UPS	Redes e Infraestructura y Servicios Informáticos	Inmediato	L4	L4
	I.9	Aseguramiento de la disponibilidad	70%	Generación de incidencia	Redes e Infraestructura y Servicios Informáticos	Inmediato	L3	L4
	I.11	Climatización	50%	Poseer salas herméticas	Redes e Infraestructura y Servicios Informáticos	Largo plazo	L2	L3
	E.23	Protección de los equipos informáticos	50%	Poseer equipos de Backup	Redes e Infraestructura y Servicios Informáticos	Corto plazo	L3	L4
	A.6	Uso de firmas electrónicas	80%	La firma electrónica es personal e intransferible	Servicios Informáticos	Inmediato	L3	L5
	A.7	Perfiles de Seguridad	60%	Usuarios invitados con restricción de perfil	Todos	Inmediato	L3	L4
	A.11	Identificación y autentificación	80%	Personal evitar divulgar o robar contraseñas.	Redes e Infraestructura	Inmediato	L3	L5

	A.23	prevención de intrusión	70%	Utilizar herramientas de prevención de intrusos en el equipo; no divulgar contraseñas	Todos	Corto plazo	L2	L4
	A.25	Control de acceso físico	60%	Evitar el ingreso a personas desconocidas; Poseer un seguro; Cámaras de vigilancia	Todos	Corto plazo	L3	L4
	A.26	Protección de las Instalaciones	50%	Poseer Data Center de emergencia	Redes e Infraestructura	Largo plazo	L2	L4
	A.27	Defensa en profundidad	50%	Poseer instalación con puertas blindadas	Redes e Infraestructura	Largo plazo	L2	L4

Fuente: (Elaboración Propia) & (PILAR, 2017)

Los resultados que se muestran en la Tabla 11 son los tratamientos o salvaguardas para cada amenaza estas deben trabajar de la mano del comportamiento ético del personal técnico y administrativo esto significa que todo procedimiento de recuperación debe tener una responsabilidad ética y profesional que permita actuar de forma inmediata ante el riesgo, los comportamientos éticos lo deben poner en práctica y conocerlos para poder mejorar el servicio que presta el Departamento de Tecnología. Por otra parte, el personal debe regirse bajo códigos de ética profesional propias del área, en la investigación se pudo determinar que existe un código de ética aprobado por el Consejo Universitario, pero al no ser divulgado y socializado se tiene poco o ningún interés por cumplir la ley. Identificar el área responsable de ejecutar la salvaguarda y en qué tiempo de respuesta se debe restituir el servicio: inmediato (1 hora a 1 día), Corto plazo (1 día a 7 días), Mediano plazo (7 días a 60 días) y Largo plazo (60 días o más). Los porcentajes de eficacia de la salvaguarda son un aproximado de la metodología MAGERIT.

Conociendo los riesgos tecnológicos también se ve la necesidad de protegerse de los riesgos personales. Para esto se debe tener un código de ética propia de las actividades y del comportamiento diario del personal que labora dentro del Departamento de Tecnología **Anexo F**. Siguiendo los estándares de la norma ISO 26000 y la ISO 37001 esta última norma se refiere al cómo evitar la corrupción en el sector público es un tema del que se debe tener mucho cuidado ya que puede afectar los objetivos, metas y la reputación propia y de la institución.

3.8 Monitoreo y revisión

Como parte del proceso de gestión del riesgo, los riesgos y los controles se deben monitorear y revisar de manera regular. Comprende definir y utilizar mecanismos para la verificación,

supervisión, observación crítica o determinación del estado de los riesgos y controles. (ISO, 2009). La herramienta PILAR nos ayuda a realizar esta monitorización con gráficos determinando el nivel del riesgo y hacia donde se debe llegar para mitigar o reducir el mismo.

3.9 Comunicación y Consulta

Comprende definir y utilizar mecanismos para comunicar y consultar con los interesados internos y externos, según resulte apropiado en cada etapa del Proceso de Gestión de Riesgos.

Debe existir formas de comunicación para mantener informada a la comunidad universitaria, la manera de comunicación de los técnicos con sus usuarios es mediante el sistema de mesa de ayuda que lo que hace es mantener informado al usuario sobre las actividades y el estado del requerimiento ante cualquier riesgo.

También se pretende asociar la mesa de ayuda con el departamento de comunicación lo que hará la mesa de ayuda es cuando el técnico de primera o segunda línea detecte que el riesgo o interrupción del servicio y su tratamiento va a tomar un mayor tiempo de recuperación pasara la información del problema, su causa, su salvaguarda y el tiempo de solución para que sea comunicada oportunamente a las autoridades y a todo el personal Universitario.

Capítulo 4

Plan de Contingencia.

4.1 Definición Plan de Contingencia

Un plan de contingencia en un Sistema de Gestión de Seguridad de la Información según la Norma ISO-27001:2013 se puede definir como: "presentación para tomar decisiones específicas cuando surja una condición que no se encuentre considerada en el proceso de planeación formal". (ISO 27001, 2013).

Por lo que es un conjunto de procedimientos que permiten la recuperación en casos de desastres, un plan formal que describe todos los pasos que se tienen que seguir en caso de que suceda una emergencia.

Tiene diferentes fases que son:

Fase de Alerta.

Fase de Transición.

Fase de Recuperación.

Fase de Vuelta a la normalidad.

4.2 Componentes de un Plan de Contingencia

Luego de la revisión de las amenazas, vulnerabilidades de los activos y sus salvaguardas, es necesario contar un Plan de Contingencias.

Trabajar solamente en la prevención es incorrecto por tres razones:

1. Es imposible asegurar que se han identificado todos los posibles orígenes de los riesgos o puntos únicos de falla, ya que se pueden tener varias combinaciones.

2. Hay riesgos que por su costo no es rentable prevenir.

3. Hay riesgos que no se pueden prevenir.

Pese a que se desarrolle un excelente Plan de Gestión de Riesgo y éticos, los riesgos igual pueden suceder.

Por todo lo mencionado es necesario trabajar en la implementación de una respuesta que permita la recuperación operativa de los activos o procesos críticos de la unidad de educación superior ante cualquier suceso previsto o no, que provoque una interrupción en las operaciones administrativas, educativas y de más actividades propias de la organización, o que la obliguen a trabajar por debajo de los estándares mínimos de calidad de servicio.

Esta respuesta será la solución de continuidad de las operaciones, la cual se ejecuta a partir de la definición de un Plan de Contingencia.

De acuerdo a la experiencia recogida por la consultora Internacional PricewaterhouseCoopers (PwC) en sus trabajos sobre planes de contingencia de las operaciones en todo el mundo, se manifiesta que, para lograr una solución real en relación a este tema, no basta con desarrollar un buen Plan de Contingencia, sino que se deben considerar de manera muy especial otros componentes fundamentales:

1. Contar con la participación y el compromiso del personal involucrado (Gestión ética). en todos los procedimientos incluidos en el Plan.

2. Disponer de la infraestructura y recursos económicos requeridos para sustentar las estrategias de recuperación que se planteen en dicho Plan.

3. Plan de Contingencia constantemente actualizado y simulacros periódicos que permita garantizar la recuperación independientemente de lo que haya sucedido.

Si se analiza los porcentajes de incidencia de cada uno de estos tres (3) componentes en el éxito que pueda alcanzar una organización al activar su Plan de Contingencia (PDC), se presenta los siguientes resultados en la Figura 12.

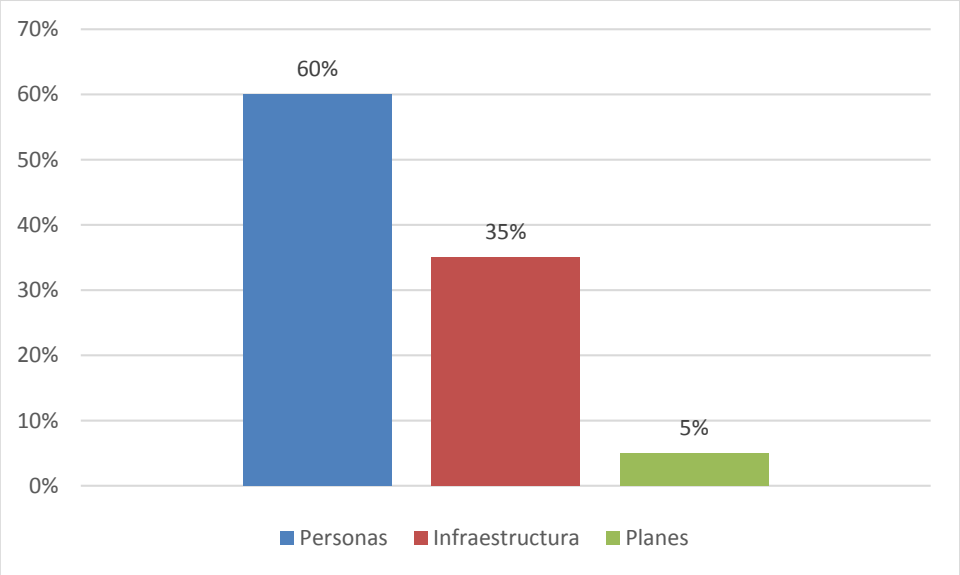


Figura 12. *Componentes fundamentales en el éxito del PDC.*
Fuente: (Elaboración Propia) & PricewaterhouseCoopers

Se puede concluir que el Personal constituye en el 60% como clave fundamental para el éxito de cualquier Plan de Gestión sea de Contingencia, riesgos o éticos.

4.3 Desarrollo del Plan de Contingencia.

4.3.1 Organización de los equipos

Previo a la ejecución de un Plan de Contingencia se debe formar los equipos, cada grupo o equipo tiene sus funciones y procedimientos que tienen que ejecutar durante las distintas fases del plan.

En el **Anexo D** se detalla la conformación de los equipos.

Los equipos son los siguientes.

Equipo Comité de Riesgos: Encargado o encargados de dirigir las acciones durante la contingencias y recuperación.

Equipo de Recuperación: Son los encargados de restablecer todos los sistemas necesarios.

Equipo Logístico: Son los responsables de toda la logística necesaria en el esfuerzo de recuperación.

Equipo de las Unidades de Negocio: Son los encargados de las pruebas que verifiquen la recuperación de los sistemas críticos.

Equipo de Relaciones Públicas: Encargados de la comunicación a los medios de comunicación y a los clientes.

"La cantidad de personal en cada uno de los equipos depende del tamaño de la organización y de la estrategia de recuperación seleccionada." (Del Pino Jimenez, 2009).

A continuación, en la Tabla 12 se presenta las actividades que tiene que cumplir cada grupo o persona involucrada en la ejecución del Plan de Contingencia.

Tabla 14
Actividades y Responsables del Plan de Contingencia

	Equipos o Responsables que intervienen en el Plan de Contingencia								
Actividades	Usuarios	Propietarios de los Procesos	Mesa Ayuda (1ra y 2da línea)	Director de Seguridad de la Información (CISO)	Comité de Riesgos	Equipo de Recuperación	Equipo Logístico	Equipo Unidades de Negocio	Equipo Relaciones Públicas
Reportar perdida de servicio	x	x							
Verificar si es un Incidente o un Problemas			x						
Incidente Resolver en 1ra 2da línea			x						
Comunicar Incidencia resuelta al Usuario			x						
Comunicar en caso de Problema			x	x					
Análisis de la Situación					x				
Decisión de activar o no el Plan de Contingencia					x				
Iniciar el Proceso de Notificación a los Responsables					x				x
Seguimiento del Proceso Recuperación					x				
Utilizar la Infraestructura y recursos para la recuperación del servicio						x			
Cubrir todas la necesidad logísticas que impliquen la recuperación.							x		
Contactar Proveedores							x		

Elaborar comunicación a los Usuarios sobre el problema			x						x
Pruebas de Funcionamiento, verificando la operatividad o restitución del servicio	x	x						x	

Fuente: (Elaboración Propia) & (ISACA, 2012).

Caso de estudio.

De acuerdo a las encuestas y al análisis de activos con mayor impacto en la organización se va a proceder con el plan de contingencia de daño en la base de datos. El escenario un usuario cualquiera de la dependencia matrícula y admisión llama a la mesa de ayuda con un error en el sistema de matrículas, este no le despliega la información del estudiante para proceder a la matrícula.

4.3.2 Fase de Alerta

Procedimiento de notificación del desastre

Cualquier usuario de la Universidad que puede reportar a la mesa de ayuda si existe un incidente que interrumpa su trabajo cotidiano, debe comunicarlo a la mesa de ayuda que determinara luego del análisis de los técnicos de primera línea y segunda línea si la incidencia puede ser resuelta en primera instancia o caso contrario se convierte en un problema o desastre que no tenga una solución inmediata es necesario informar al Director de Seguridad proporcionando el mayor detalle posible en la descripción de los hechos.

"El Director de Seguridad debe evaluar la situación y si amerita informar al Responsable del Comité de Riesgos para la evaluación se debe tener presente estos criterios". (Carrizo, Alfaro, & Loyola, 2016).

Tabla 15
Tipos de Desastres

Tipo Desastre	Descripción	Acción.
Desastre menor	Aquel que provoca una parada que no sobrepase las dos horas establecidas como mínimo.	Comunicar a la mesa de ayuda que resuelva el problema
Desastre mayor	Aquel que provoca una parada de más de dos horas y que no sobrepase las horas hábiles de trabajo.	Comunicar a la mesa de ayuda y mantener informado al Representante del Comité de riesgos
Desastre Catastrófico	Cuando el sistema informático vaya a estar fuera de servicio más de las horas hábiles o fuera del horario normal de trabajo.	Comunica al Comité de Riesgos

Fuente: (Elaboración Propia) & (Carrizo, Alfaro, & Loyola, 2016)

Procedimiento de ejecución del Plan

El Comité de Riesgos reunido en el punto de encuentro evaluará la situación. Con toda la información de detalle sobre el incidente, se decidirá si se activa o no el Plan de Contingencia. En caso afirmativo, se iniciará el procedimiento de ejecución del Plan.

En el caso de que el Comité decidida no activar el Plan de Contingencia porque la gravedad del incidente no lo requiere, en este caso será necesario gestionar el incidente para que no aumente su gravedad esto lo puede resolver la mesa de ayuda con técnicos de primera y segunda línea.

Procedimiento de notificación de ejecución del plan

Activar el árbol de llamadas para avisar a los integrantes de los diferentes equipos que van a participar en el Plan. Vea el Figura 13.

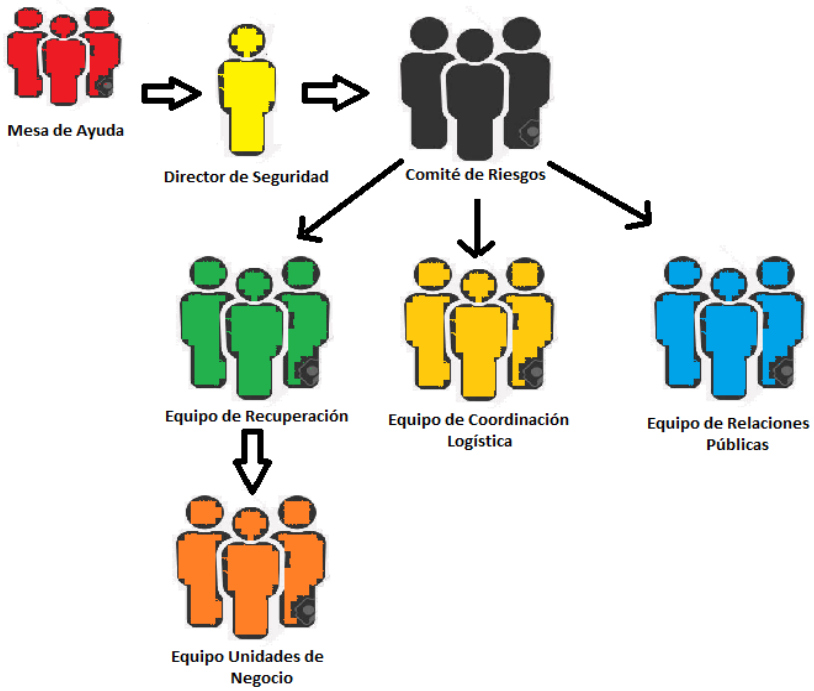


Figura 13. *Equipos para ejecutar el PDC.*
(Fuente: Autor) & (Del Pino Jiménez, 2009)

4.3.3 Fase de Transición

Procedimiento de Concentración y traslado de material y personas.

Una vez avisados los equipos y puesto en marcha el Plan, deberán acudir al centro de reunión indicado. Además del traslado de personas al lugar del problema lo más usual es que sea al Data Center hay que trasladar todo el material necesario o que solicite el equipo de Recuperación para poner en marcha el centro de recuperación (cintas de backup, servidor de respaldo, discos externos, NAS). Esta labor tiene que ser trabajado simultáneamente con el equipo logístico por lo que es recomendable tener el listado de proveedores con sus números de contacto y correos electrónicos como en la siguiente tabla.

Tabla 16
Equipos para ejecutar el PDC.

Proveedores			
Proveedor	Equipos	Teléfono	Contacto.
Coresolutions	Servidores IBM	450022	henry@coresolutions.com
Compuhelp	Impresoras HP	4700033	luis.loja@holydat.com
Ecuacopia	Impresoras Ricoh	456789	cristian.avila@ecuacopia.com
Repycom	Equipos HP	417070	mercedes.s@repycom.com
Coresolutions	Cisco	450022	luis@coresolutions.com

Fuente: (Elaboración Propia)

Procedimiento de puesta en marcha del centro de recuperación

Una vez que el equipo de recuperación llegue al Data Center y que los materiales empiecen a llegar, pueden comenzar a realizar el listado de requerimientos para cumplir con los tiempos de recuperación.

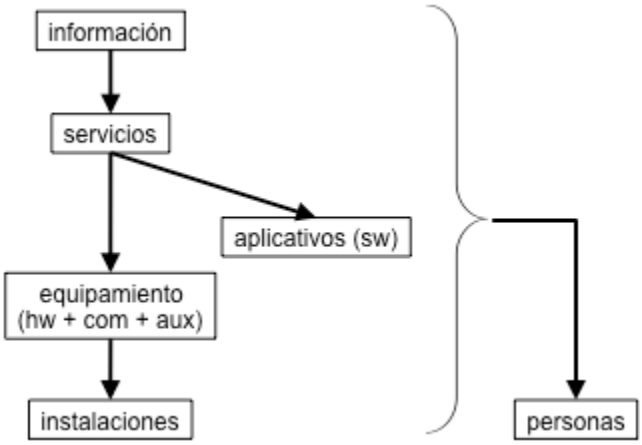


Figura 14. *Jerarquía de Dependencias de activos.*
Los activos o servicios para sus requerimientos se necesita saber sus dependencias tanto físicas como lógicas.
Fuente: MAGERIT (2012)

El equipo de recuperación solicitará al equipo de logística cualquier tipo de material extra que fuera necesario para la recuperación por eso se tendrá el siguiente registro detallado en la siguiente Tabla.

Tabla 17
Requerimiento Interno para el PDC.

Requerimiento Interno								
Fecha	Activo	Características	Actividad	Código Inventario	Ubicación	Tiempo esperado	Tiempo Real Restitución	Responsable
12/12/2017	Servidor	IBM Procesador XEON 2,3 GHZ, 16 GB RAM; 2 TB D.D	Activar servidor provisional	109789	Data Center	15 min	15 min	Ing. Darío P.
12/12/2017	Windows Server	Windows Server	Instalar Sistema Operativo	130502	Servicios Informáticos	30 min	2 Horas	Ing. Eduardo B.
12/12/2017	Backup	Backup Base de Datos	Recuperar Backup	xxx	Data Center	2 Horas	4 Horas	Ing. Pablo O.
						Total Tiempo	6:15 Horas	

Nota: El Requerimiento interno se ejecuta de activos que sean dependientes del activo que presento la catástrofe.
Fuente: (Elaboración Propia) & (Universidad, 2017).

4.3.4 Fase de Recuperación

Procedimiento de restauración

El orden de recuperación de las funciones se realizará según la criticidad de la Base de Datos: Se realizará un listado de los requerimientos internos o lo que posee la institución y requerimientos externos que se necesite de proveedores. En el **Anexo E** se muestra el registro

que tiene que ser llevado en estos procedimientos con los siguientes campos: la causa del problema para el ejemplo de la Base de Datos, su criticidad, y de más datos que fueron recogidos de experiencias del área de Servicios Informáticos. Los tiempos de respuesta dependerán si son requerimientos que posee la Institución ósea internos o se necesita la intervención de proveedores requerimientos externos.

Procedimiento de soporte y gestión

Una vez recuperados los activos, se avisará a los equipos de los departamentos que gestionan los sistemas (listado del equipo de Unidades de Negocio) para que realicen las comprobaciones necesarias que certifiquen que funcionen de manera correcta y pueda continuarse dando el servicio.

Además, el Equipo o el Director de Seguridad deberá comprobar que existen las garantías de seguridad necesarias (confidencialidad, integridad, disponibilidad) antes de dar por terminada la fase de recuperación.

4.3.5 Fase de vuelta a la normalidad

Una vez con los procesos críticos en marcha y solventada la contingencia, hay que plantearse las diferentes estrategias y acciones para recuperar la normalidad total de funcionamiento.

Análisis del impacto

Es el momento de realizar una valoración detallada de los equipos e instalaciones dañadas para definir la estrategia de vuelta a la normalidad. Para ello, el equipo de recuperación junto con el equipo de seguridad, realizarán un listado de los elementos que han sido dañados gravemente y son irrecuperables, así como de todo el material que se puede volver a utilizar.

Esta evaluación deberá ser comunicada lo antes posible al equipo Comité de riesgo para que determinen las acciones necesarias que lleven a la operación habitual lo antes posible.

Adquisición de nuevo material

Una vez realizada la evaluación del impacto, se determinará la necesidad de nuevo material. El Comité de Riesgo contactará con el seguro de la compañía para conocer qué parte cubre el seguro (dependiendo del tipo de póliza contratada por la Universidad.) y qué inversión tendrá que hacer la compañía en el material que no se pueda recuperar.

Contactar con los proveedores para que en el menor tiempo posible repongan todos los elementos dañados vea la Tabla 16.

Tabla 18
Requerimiento Externo para el PDC

Requerimiento Externo								
Fecha	Requerimiento Externo	CAUSA	Reposición	Valor	Tiempo entrega	PROVEEDOR	TELEFONO	Responsable
12/12/2017	Servidor	Servidor Quemado	G	0	30 días	Coresolutions	406000	Ing. Diego P.
				Total Tiempo	30 días			

Nota: Reposición: G: Garantía; S: Seguro; C: Compra.
Fuente: (Elaboración Propia)

4.3.6 Fin de la contingencia

Dependiendo de la gravedad del incidente, la vuelta a la normalidad de operación puede variar entre unos días (si no hay elementos clave afectados) e incluso meses (si hay elementos clave afectados). Lo importante es que, durante el transcurso de este tiempo de vuelta a la

normalidad, se siga dando servicio a los usuarios por parte de la organización y que la incidencia afecte lo menos posible a la Institución. El equipo de comunicación debe siempre mantener informado a los usuarios y los equipos deben estar constantemente informando al Comité de Riesgo.

Conclusiones y Recomendaciones

Es importante contar con un plan de gestión de riesgos tecnológicos que sirva como guía para todas las organizaciones educativas y que el departamento de tecnología tenga la suficiente información sobre cómo actuar ante los riesgos tecnológicos críticos con un Plan de Gestión de Riesgos y de Contingencia y poder seguir los lineamientos de una metodología clara que cumpla los estándares internacionales del proceso de gestión del riesgo. La metodología contiene varios pasos que con la ayuda de herramientas como PILAR sirvieron en la implementación de la metodología MAGERIT. Con el Plan de gestión de riesgos en conjunto con la ética se puede determinar que activos tienen mayor vulnerabilidad contra el riego y que impacto ocasionaría su ausencia en la organización con esto se prioriza y se identifica sus salvaguardas, responsabilidades y el tiempo de respuesta para la solución. El uso de la herramienta PILAR, las encuestas y la lluvia de ideas del personal experto en cada área, ayudo a obtener los resultados y a entender mejor la implementación de la metodología de forma cualitativa.

Con esta investigación se presenta un ejemplo práctico con la propuesta de Gestión de riesgos y éticos ya que existe mucha información de normas y metodologías que uniéndolas tomando lo más relevante y poniéndolo en práctica en un caso de estudio real se puede adaptar proponiendo una metodología que se acople a las necesidades de la Institución y que sirva como referente para otras organizaciones públicas o privadas.

En el desarrollo del trabajo se pudo obtener la identificación de los riesgos más críticos que por su impacto y probabilidad ponen en riesgo a la Institución. Al identificar los riesgos se pueden mitigar los mismos con las salvaguardas y responsabilidades éticas. El código y

comportamiento ético no debe ser un tema aparte del Plan de Gestión del riesgo por esto se propuso incluir en el tratamiento del riesgo. Por otra parte, los riesgos catastróficos deben ser tratados inmediatamente y estar preparados con el plan de contingencia del riesgo que presente mayor criticidad de acuerdo a los resultados obtenido de PILAR y del resultado de las encuestas.

En cuanto a los trabajos futuros, se pretende abarcar la mayor cantidad de riesgos tecnológicos dentro del departamento, aprobar un código de ética para que el personal cumpla con estándares internacionales de comportamiento ético y de responsabilidad social. Se puede tener un excelente plan de gestión del riesgo, pero si no existe un código de ética que permita tener un personal que cumpla sus deberes y obligaciones en sus labores de gestión, se volverá al estado anterior en donde se desconoce y no se pone en práctica ningún plan de gestión por más importante que sea. Esto permitirá definir un proceso del riesgo que en conjunto con la gestión ética permitirá cumplir con los objetivos no solo del departamento de tecnología sino también de la institución.

Las principales recomendaciones se tienen las siguientes:

Mejorar la estructura organizativa del Departamento de Tecnología, se debe contar con una coordinación de seguridad.

Iniciar el proceso de socialización del Plan propuesto para que sea implementado y ejecutado, no se debe permitir el desconocimiento de dichos planes.

Subir los niveles de tratamiento del riesgo a un nivel óptimo o aceptable, en la investigación se puede apreciar que en ciertos riesgos no se posee ninguna salvaguarda que ayuden a contrarrestarlos.

El personal al tener bastante rotación si bien tiene conocimientos y realiza su trabajo de forma empírica o práctica, se deben tener procedimientos, políticas y planes al alcance de ellos para utilizarlos y socializarlos con esto agilitar los tiempos de respuesta.

Se debe asignar responsables y dueños del proceso de tratamiento de los riesgos y en la ejecución del plan de contingencia.

Se debe de cumplir con los tiempos óptimos y constantemente en la práctica reducirlos para restituir los servicios en el menor tiempo con esto se evita perdidas económicas

La alta Gerencia debe estar comprometida y apoyar al Departamento de Tecnología en la ejecución de estos planes de Gestión que lo único que hacen es dar un valor agregado a la Universidad y ante la sociedad.

El personal también debe estar comprometido en la correcta ejecución del Plan de Gestión del Riesgo y ético, el 60% de éxito depende del personal.

En cuanto a costos deben ser acordes a las posibilidades de la Institución habrá activos que pueden ser protegidos con costos bajos inmediatamente, pero hay activos como un Data Center de emergencia que representan costos muy altos. Por lo que se debe hacer un estudio de factibilidad y presupuesto para la adquisición o arrendamiento. Esto no se debe de ver como gasto más bien como inversión a largo plazo.

Glosario de términos.

(A) Ataques deliberados: Fallos deliberados causados por las personas.

(E) Errores y Fallos no Intencionados: Según MAGERIT (2012) son errores causados por el ser humano sin intensión.

(I) Desastre Industrial: Según MAGERIT (2012) son amenazas que pueden darse de cualquier forma deliberada o accidental provocada por el Hombre de tipo industrial.

(N) Desastre Naturales: Según MAGERIT (2012) cualquier suceso que pueda ocurrir directa o indirectamente sin la participación del ser humano.

Activo Intangible: Es definido por su propio nombre, es decir, no es tangible, no puede ser percibido físicamente por ejemplo Un Sistema

Activo Tangible: Tiene una forma física, es decir, son activos materiales que se pueden ver y tocar por ejemplo un Computador.

Amenaza: Cosa o persona que constituye una posible causa de riesgo o perjuicio para alguien o algo.

Antivirus: Programa que detecta la presencia de un virus informático en un disco, memoria o en una computadora y lo elimina.

Código Fuente: El código fuente de un programa está escrito por un programador en algún lenguaje de programación, pero en este primer estado no es directamente ejecutable por la computadora, sino que debe ser traducido a otro lenguaje.

Copias de respaldo: Son duplicados que son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar

una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas.

Data Center: es, tal y como su nombre indica, un "centro de datos" o "Centro de Proceso de Datos" (CPD). Esta definición engloba las dependencias y los sistemas asociados gracias a los cuales: Los datos son almacenados, tratados y distribuidos al personal o procesos autorizados para consultarlos y/o modificarlos.

Datos Institucionales: Son datos o información esenciales para la Institución.

DT: Departamento de Tecnología es el departamento responsable de llevar a cabo todas las actividades relacionadas con la planificación, definición de estrategias, dirección y arquitectura de tecnologías de la información.

Gestión Ética: Permite incorporar de manera práctica los valores organizacionales tanto en la estrategia como en sus operaciones cotidianas

Gestión Riesgo Tecnológico: Es la Gestión para prevenir las pérdidas potenciales por daños, interrupción, alteración o fallas en el funcionamiento u operación, derivadas del uso o dependencia de equipos, sistemas de distribución, productos y demás componentes de la tecnología

Impacto: Consecuencia que se genera de la materialización de un riesgo.

MAGERIT: Según MAGERIT (2012) "Es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica Español para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas."

Mesa de Ayuda: Se basa en un conjunto de recursos técnicos y humanos que permiten dar soporte a diferentes niveles de usuarios informáticos de una empresa, tales como: Servicio de soporte a usuarios de "sistemas microinformáticos" Soporte telefónico centralizado en línea (on-line)

Ofimática: Conjunto de materiales y programas informáticos que se aplican al trabajo de oficina. Ejemplo Microsoft Office

PDC Plan de Contingencia: es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas.

PILAR: Es una herramienta utilizada para implementar la metodología MAGERIT analiza los riesgos en varios frentes: disponibilidad, confidencialidad, integridad, autenticidad, trazabilidad y valor.

Primera Línea: Es el personal tecnológico que asiste en primera instancia vía telefónica o personal ante cualquier incidente tecnológico de los usuarios.

Probabilidad: Probabilidad que tiene un riesgo de materializarse.

Riesgo: Posibilidad de que se produzca un contratiempo o una desgracia, de que alguien o algo sufra perjuicio o daño.

Salvaguarda: Son recursos o acciones que permiten hacer frente a las amenazas.

Segunda Línea: Es el personal tecnológico especializado que asiste en segunda instancia vía telefónica o personal ante cualquier incidente tecnológico de los usuarios

Servidor de Aplicaciones: Usualmente se trata de un dispositivo de software que proporciona servicios de **aplicación** a las computadoras cliente. Un servidor de aplicaciones

generalmente gestiona la mayor parte (o la totalidad) de las funciones de lógica de negocio y de acceso a los datos de la aplicación.

Servidor: Es un ordenador físico en el cual funciona software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.

Sistemas de Gestión de Base de Datos: (SGBD) es un conjunto de programas que permiten el almacenamiento, modificación y extracción de la información en una base de datos, además de proporcionar herramientas para añadir, borrar, modificar y analizar los datos.

Voto electrónico: es una expresión que comprende varios tipos de votación, que abarca tanto modos electrónicos de emitir votos (**voto** por internet) como medios electrónicos de contar los votos. ... También puede referirse a la transmisión de papeletas y votos por vía telefónica, redes de computación privadas o por Internet

Bibliografía

Argandoña, A., & Isea, R. (Junio de 2011). *ISO 26000, UNA GUIA PARA LA RESPONSABILIDAD SOCIAL DE LAS ORGANIZACIONES.* Obtenido de http://www.iese.edu/es/files/catedralacaixa_vol11_final_tcm5-72287.pdf

Calle , G. (1996). *Reingeniería y seguridad en el ciberespacio.* Madrid: Díaz de Santos.

Carrillo, J. (2013). Gestión del riesgo en las metodologías de proyectos de tecnologías de información y comunicaciones. *ENFOQUEUTE*, 77-94.

Carrizo, D., Alfaro, A., & Loyola, R. (2016). PROPUESTA DE UN MODELO DE PLAN DE CONTINUIDAD: UN ESTUDIO DE CASO. *Memorias de la Décima Quinta Conferencia Iberoamericana en Sistemas, Cibernética e Informática*, (pág. 6). Chile.

Del Pino Jimenez, L. (Marzo de 2009). *Guía de Desarrollo de un Plan de Continuidad de Negocio.* Obtenido de http://www.criptored.upm.es/guiateoria/gt_m001r.htm

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* . Madrid: Ministerio de Hacienda y Administraciones Públicas.

Espinoza, D., Martínez, J., & Siler, A. (2014). Gestión del riesgo en la seguridad de la información con base en la Norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la Metodología OCTAVE-S. Caso de estudio: proceso de inscripciones y admisiones en la división de admisión registro y control AC. *Revista de Ingenierias USBMED*, 33-43.

Gaona, K. (10 de 2013). *APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS Y*. Obtenido de http://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf

Heredero, P. (2006). *Dirección y gestión de los sistemas de información en la empresa : una visión integradora.* Madrid: ESIC.

ISACA . (2016). *ISO 37001*.

ISACA. (2012). *Cobit 5.* EEUU: ISACA.

ISO. (1 de 11 de 2011). *ISO 31000*. Obtenido de https://www.iso.org/iso-31000-risk-management.html

ISO 27001. (2013). *ISO/IEC 27001:2013*. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Miranda, M. F. (2015). *Propuesta de un Plan de Gestión de Riesgos de Tecnologia Aplicado a la Escuela Politecnica Superior del Litoral.* Obtenido de http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

NTC-ISO 31000. (16 de 02 de 2011). *Gestión del Riesgo Principios y Directrices*. Obtenido de Norma Tecnica Colombiana: https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf

NTE-INEN-ISO 31000. (04 de 2014). *GESTIÓN DEL RIESGO INEN*. Obtenido de http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2014/09/31000-EXT.pdf

PILAR. (2017). Obtenido de http://www.ar-tools.com/es/tools/pilar/v62/index.html

Ramírez Castro, A., & Ortiz Bayona, Z. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la. *Ingenieria*, 56-66.

Secretaría Gestión de Riesgos. (2015). *Resolución SGR-029-2015*. Obtenido de http://www.gestionderiesgos.gob.ec/wp-content/uploads/downloads/2015/03/Resoluci%C3%B3n-SGR-029-2015.pdf

Universidad. (2017). Datos Institucionales. Cuenca, Azuay, Ecuador.

Wyman, O. (2017). *Informe de riesgos mundiales 2017*. Obtenido de http://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2017/jan/Global-Risk-Report-2017_ES.pdf

ANEXOS

Anexo A. Formato de Encuesta para evaluar la Situación Actual

Formato utilizado en las encuestas para obtener la información complementando con reuniones y lluvia de ideas para la elaboración de la investigación.

Encuesta
Gestión de Riegos Tecnológicos y Gestión ética.

Dependencia: Dirección de Tecnologías de Información y Comunicación.
Orientado al personal que labora en la Dependencia.
Encuestador: Ing. Eduardo Bernal.
Fecha: ……
Señale con una x la respuesta correcta.
Coordinación al que pertenece: Sistemas de Información: ( ), Redes e Infraestructura: ( ), Servicios Informáticos ( ).
"Entendiéndose por riesgo tecnológico cualquier activo tangible o intangible informático que impida la continuidad del negocio. Ejemplo de riesgo tecnológico: Daño en la Base de Datos."

1. **¿En su lugar de trabajo existe un plan de gestión de riesgos tecnológicos?**

SI ( ) NO ( ) Desconoce ( )

Si su respuesta es afirmativa señale cuales :
……..……
……
……
……
……

2. **¿Según su criterio señale 5 o más riesgos tecnológicos que por su importancia se podría gestionar en su Coordinación y valore su impacto en la organización siendo?**

5. Riesgo Extremo, **4**. Riesgo Alto, **3**. Riesgo Medio, **2**. Riesgo Bajo, **1**. Riesgo Leve.

Riesgos Tecnológicos	Impacto. (5,4,3,2,1)
1.	
2.	
3.	
4.	
5.	
6.	

3. **¿En su lugar de trabajo existe un plan de contingencia para mitigar los riesgos tecnológicos?**

SI ( ) NO ( ) Desconoce ( )

Si su respuesta es afirmativa señale cuales :
……..……

……
……
……
……

4. **¿De los riesgos tecnológicos citados por Usted anteriormente seleccione dos de mayor importancia que deberían de tener un plan de contingencia en el caso de ocurrir el riesgo?**

Riesgos Tecnológicos que por su importancia deberían tener un Plan de Contingencia.
1.
2.

5. **¿En su lugar de trabajo existe Políticas de Seguridad Informática?**

SI ( ) NO ( ) Desconoce ( )

Si su respuesta es afirmativa señale las que conoce:

……..……
……
……
……
……

6. **¿En su lugar de trabajo existe Políticas de comportamiento ético?**

SI ( ) NO ( ) Desconoce ( )

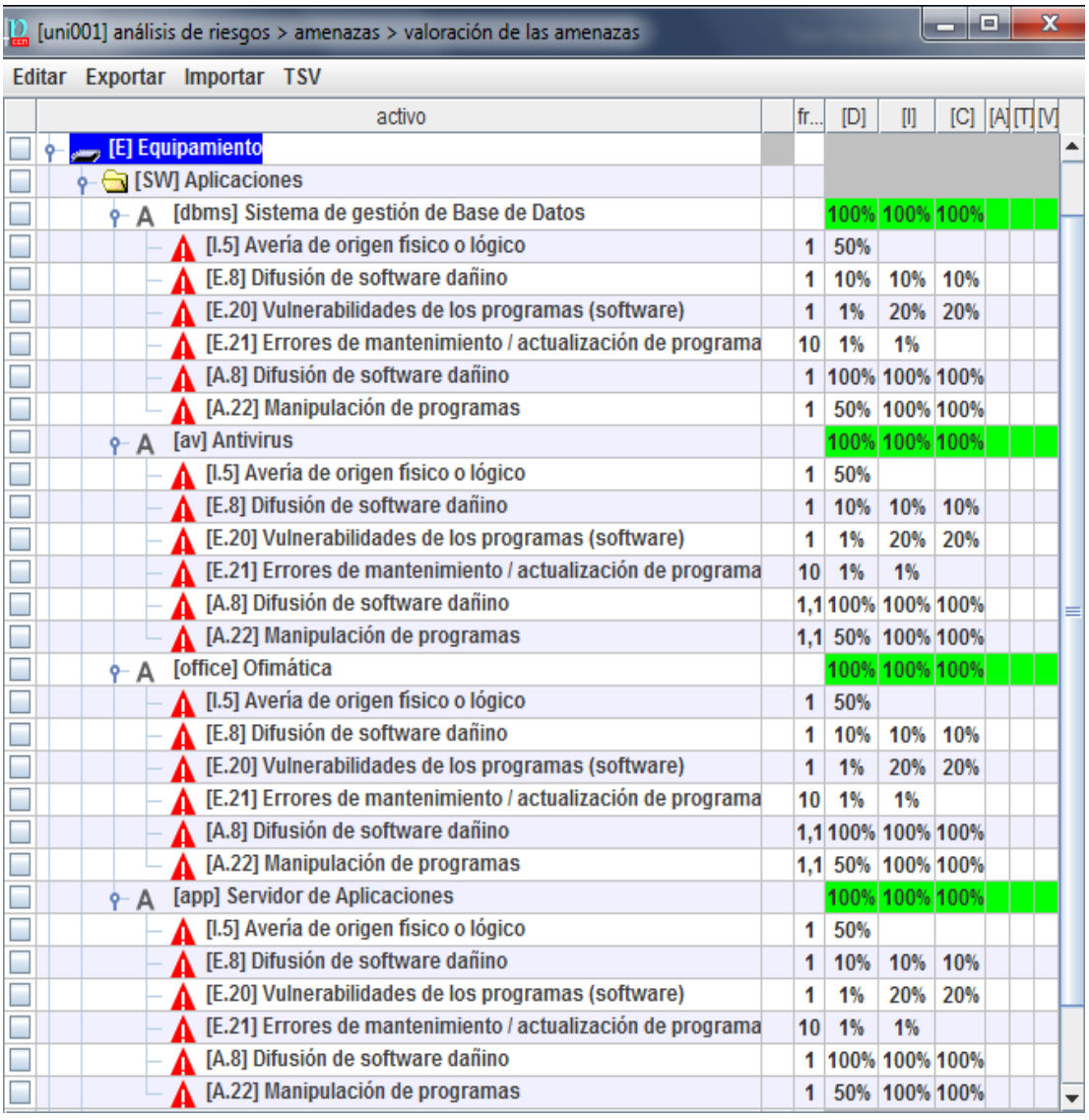
Si su respuesta es afirmativa señale las que conoce :

……..……
……
……
……
……

Gracias por su colaboración y su valioso tiempo dedicado a contestar esta encuesta sus datos son de absoluta reserva y serán utilizados para el desarrollo de un Plan de Gestión de Riesgos Tecnológicos ISO 31000 y de Políticas de Comportamiento ético ISO 37000. Hasta una próxima oportunidad muchas gracias.

Anexo B. Valoración de las amenazas utilizando la herramienta PILAR

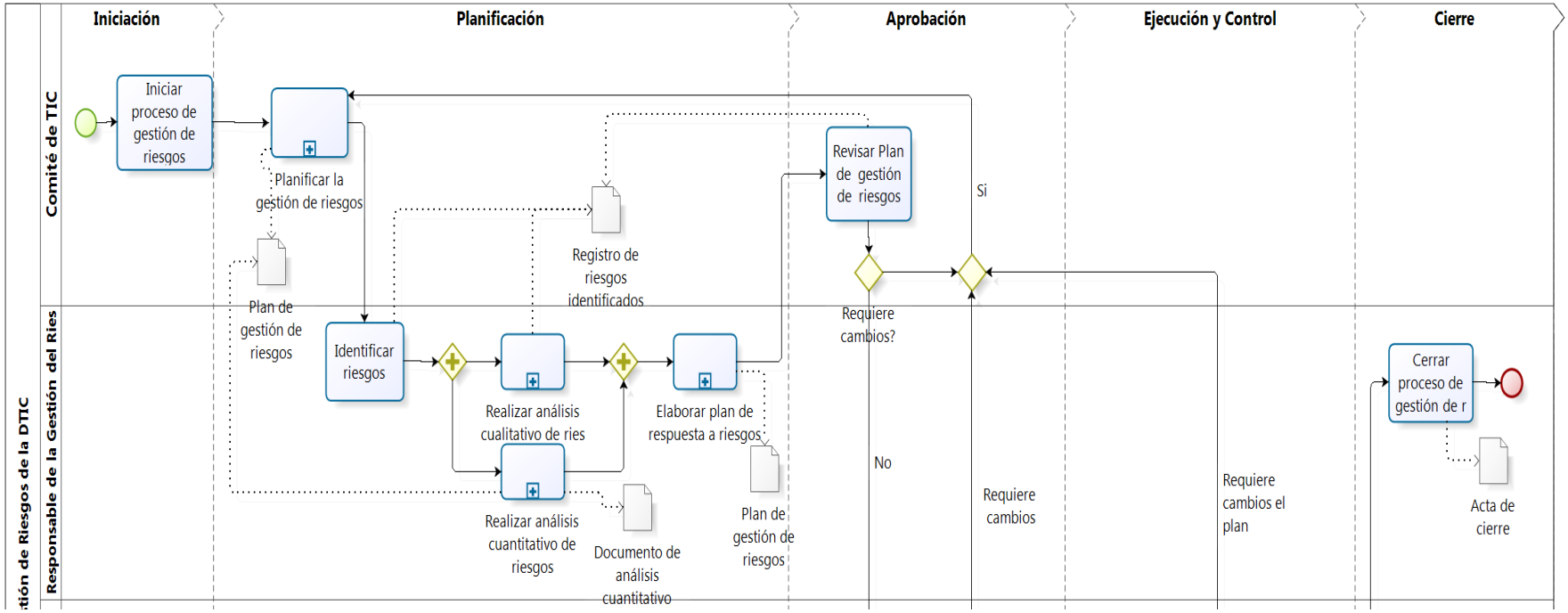
Este es un ejemplo de cómo se puede valor las amenazas utilizando datos de las encuestas ingresando en la herramienta PILAR.

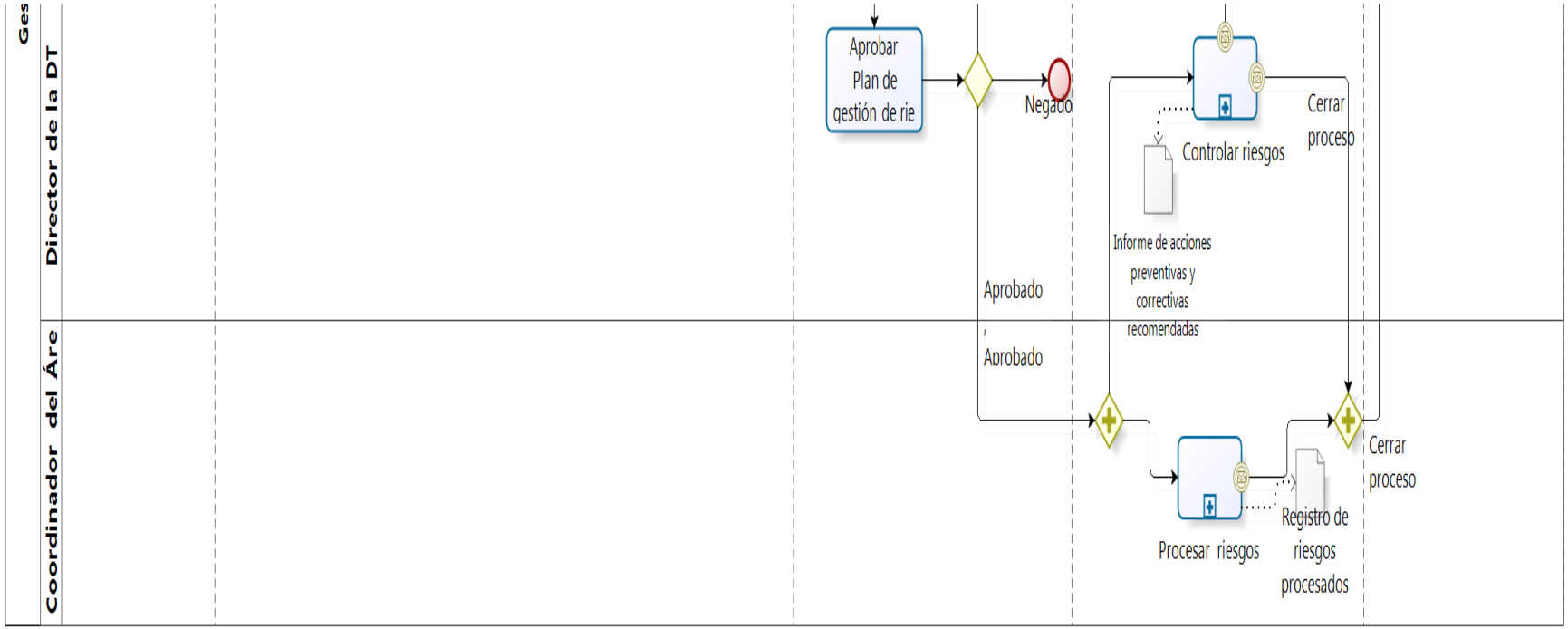


activo	fr...	[D]	[I]	[C]	[A]	[T]	[V]
[E] Equipamiento							
[SW] Aplicaciones							
A [dbms] Sistema de gestión de Base de Datos		100%	100%	100%			
[I.5] Avería de origen físico o lógico	1	50%					
[E.8] Difusión de software dañino	1	10%	10%	10%			
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%			
[E.21] Errores de mantenimiento / actualización de programa	10	1%	1%				
[A.8] Difusión de software dañino	1	100%	100%	100%			
[A.22] Manipulación de programas	1	50%	100%	100%			
A [av] Antivirus		100%	100%	100%			
[I.5] Avería de origen físico o lógico	1	50%					
[E.8] Difusión de software dañino	1	10%	10%	10%			
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%			
[E.21] Errores de mantenimiento / actualización de programa	10	1%	1%				
[A.8] Difusión de software dañino	1,1	100%	100%	100%			
[A.22] Manipulación de programas	1,1	50%	100%	100%			
A [office] Ofimática		100%	100%	100%			
[I.5] Avería de origen físico o lógico	1	50%					
[E.8] Difusión de software dañino	1	10%	10%	10%			
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%			
[E.21] Errores de mantenimiento / actualización de programa	10	1%	1%				
[A.8] Difusión de software dañino	1,1	100%	100%	100%			
[A.22] Manipulación de programas	1,1	50%	100%	100%			
A [app] Servidor de Aplicaciones		100%	100%	100%			
[I.5] Avería de origen físico o lógico	1	50%					
[E.8] Difusión de software dañino	1	10%	10%	10%			
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%			
[E.21] Errores de mantenimiento / actualización de programa	10	1%	1%				
[A.8] Difusión de software dañino	1	100%	100%	100%			
[A.22] Manipulación de programas	1	50%	100%	100%			

Anexo C. Proceso Gestión Riesgos.

Datos obtenidos de la Universidad del Proceso Gestión de Riesgos realizado en BIZAGE.




Director de la DT
Coordinador del Áre
Aprobar Plan de gestión de rie
Negado
Aprobado
Aprobado
Controlar riesgos
Informe de acciones preventivas y correctivas recomendadas
Cerrar proceso
Procesar riesgos
Registro de riesgos procesados
Cerrar proceso

Anexo D Integrantes Grupos Plan de Contingencia.

Este formato permitirá tener identificado a los equipos que intervienen en el Plan de Contingencia identificando su ubicación vía telefónica o electrónica. Para poder actuar de forma inmediata ante una catástrofe tecnológica.

Integrantes Comité de Riesgos					
Designación	Cargo	Nombre	Celular	Tel Casa	Correo
Responsable del comité	Dir. Informática	Vinicio S.	0999980930	4011000	vinicio.s@universidad.com
Miembros del Comité	Dir. T. Humano	Pedro M.	0894938388	4021000	pedro.m@universidad.com
	Dir. Financiero	Cecilia V.	0994562345	4031000	cecili.v@universidad.com
Integrantes Equipo Recuperación					
Designación	Cargo	Nombre	Celular	Tel Casa	Correo
Responsable del equipo	Coord. Redes	Jorge E.	0994560930	4041000	jorge.e@universidad.com
Miembros del equipo	Ing. Sistemas	Darío P.	0894679388	4051000	dario.p@universidad.com
	Ing. Sistemas	María M.	0991234345	4061000	maria.m@universidad.com
Integrantes Equipo Logística					
Designación	Cargo	Nombre	Celular	Tel Casa	Correo
Responsable del equipo	Coord. Servicios	Carlos M.	0994220930	4041000	carlos.m@universidad.com
Miembros del equipo	Ing. Sistemas	Eduardo A.	0845679388	4051000	eduardo.a@universidad.com
	Ing. Sistemas	Diana E.	0991234485	4061000	diana.e@universidad.com
Integrantes Equipo Relaciones Públicas					
Designación	Cargo	Nombre	Celular	Tel Casa	Correo
Responsable del equipo	Dir. Comunicación	Silvana M	0994270130	4071000	silvana.m@universidad.com
Miembros del equipo	Lic. Periodismo	José P.	0894679388	4081000	jose.p@universidad.com

Integrantes Equipo Unidades de Negocio					
Designación	Cargo	Nombre	Celular	Tel Casa	Correo
Responsable del equipo	Dir. Mat y Admisión	Natalia B.	0994512345	4091000	nathalia.b@universidad.com
Miembros del equipo	Ing. Sistemas	Susana P.	0894679388	4010000	susana.p@universidad.com
	Ing. Sistemas	Pablo C.	0991234345	4011000	pablo.c@universidad.com

Nota: Cada equipo debe tener identificado cuáles son sus miembros y como poder ubicarlo en el menor tiempo posible ante una catástrofe. También se debe definir el Centro de Reunión cercano al lugar del problema.

Centro de Reunión.

Sala de reuniones del Departamento de Tecnologías. Caso de desastre natural el Centro de Reunión será la casa del responsable del comité de riesgos Av. Solano y Remigio Crespo 1-17.

Anexo E. Procedimiento de Restauración.

Procedimiento de Restauración										
Fecha	Proceso	Estado Funcionamiento	Problemas	Causa	Solución	Criticidad	Requerimiento Interno. Solución Provisional	Requerimiento externo Solución Definitiva	Ubicación	Responsable
12/12/2017	Matricula	No muestra información del estudiante	No reconoce la Base de Datos	Servidor de Base de Datos Quemado	Cambio de Servidor y subir respaldo Base Datos	1	Servidor de Backup, Windows Server y Backup B.D.	Reposición Servidor	Data Center	Ing. Darío P.
Criticidad: 1 Alto 2 Medio 3 Bajo										

Nota: Este anexo permite tener la información necesaria para restituir el servicio necesitando Requerimiento Internos o Externos, Criticidad y Ubicación asignando un responsable. Para poder dar una solución definitiva es importante conocer que activos dependen del activo que tienen alguna criticidad.

Anexo F. Código de ética para los riesgos tecnológicos.

Este Código de Ética tiene como objeto establecer, principios, valores y normas de conducta más generales que orientan la vida diaria de los empleados del Departamento de Tecnología para cumplir con sus deberes morales y éticos en la práctica diaria.

- El personal del Departamento de Tecnología debe tratarse con respeto y cordialidad en su área de trabajo y hacia los usuarios.
- Los valores de honestidad, respeto, capacidad deben ser hábitos de la práctica diaria.
- El personal debe proteger datos importantes encriptando o tener la información en la nube.
- Restituir el backup utilizando el Plan de Contingencia cuando ocurra algún desastre en cualquier activo tangible o intangible relevante para la Universidad.
- Evitar divulgar o robar contraseñas por cualquier medio físico o electrónico.
- Evitar plagios o falsificar los accesos suplantando identidades o permisos (DATA CENTER).
- Alterar información relevante de forma deliberada en la base de datos.
- Poner en práctica el anti soborno a toda la comunidad Universitaria Docentes, estudiantes, empleados que pongan en riesgo la ética profesional.
- La utilización de la firma electrónica es personal e intransferible en cualquier documento electrónico.
- No permitir el ingreso al DATA CENTER sin identificación o con autorización de la Coordinación de Redes e Infraestructura.
- Mantener los equipos con protección eléctrica conectar correctamente los UPS,

Generadores eléctricos.

- Ejecutar el antivirus una vez por semana; Levantar los Firewall. No abrir correos maliciosos.
- Configurar perfiles de seguridad en el dominio parches y antivirus.
- Personal ejecutar parches y actualizaciones de los programas mediante el Dominio para evitar vulnerabilidades en el software.
- No permitir la manipulación de programas en producción. Se debe tener una base de datos en producción y otra de pruebas.
- Utilizar extintores de espuma para equipo informático que no dañe los componentes de los equipos en caso de incendio.
- Evitar el paso de tuberías de agua cerca de equipos en especial cerca del DATA CENTER.
- Poseer equipos de Backup y listas de proveedores cuando el Plan de Contingencia lo amerite.
- El personal que administra el DATA CENTER debe sugerir que cumpla con todas las normas de seguridad.
- Supervisar el correcto funcionamiento y el mantenimiento respectivos de Generadores eléctricos y UPS.
- Supervisar el correcto funcionamiento y el mantenimiento respectivos de los ductos de climatización para tener la temperatura ideal del DATA CENTER.
- Realizar levantamientos periódicos de los activos que posee la Universidad con el fin de reponer equipos que ya cumplieron su vida útil.

- Asegurar equipos que por su valor e importancia permita la reposición contra perdidas de equipos.
- Brindar el servicio de wifi con mejor cobertura y con contraseña para evitar la subutilización de personal que no pertenezca a la Universidad.
- Definir perfiles de Usuarios como invitados con restricción en la utilización de equipos.
- Utilizar herramientas de prevención de intrusos en los equipos.
- Poseer Cámaras de vigilancia que ayuden a cuidar de cualquier ataque o robo a personas o a bienes físicos.
- El personal de Infraestructura debe tener un proyecto de mejora o de respaldo de infraestructura como un DATA CENTER de emergencia.
- Poseer manuales para los usuarios en la utilización de los servicios y sistemas que presta la Universidad
- Recibir capacitaciones para mejorar el servicio.
- Difundir a todo el personal el plan de Gestión de Riesgos y Gestión ética.
- Realizar pruebas periódicas y actualizar constantemente el Plan de Contingencia.
- Capacitar al personal en valores, actualización de conocimientos y en atención al cliente.
- Realizar encuestas de satisfacción a los usuarios que utilizan los servicios informáticos.
- Evitar bajo ningún motivo recibir coimas en cualquier proceso de compra de bienes.

Anexo G. Fórmula para calcular la muestra.

Fórmula

$$n = \frac{N.Z^2.p.q.}{(N-1)\,e^2 + Z^2.p.q.}$$

n=Tamaño de la muestra

N= Tamaño de la Población (Ingenieros de Sistemas 32)

P= la probabilidad de ocurrencia de la variable principal en estudios es igual a 0.5

q. La probabilidad de no ocurrencia de la variable principal en estudio que igual a 0.5

e= nivel de error esperado, que expresado en porcentaje es el 5% (0.05).

Z= nivel de confianza, para un nivel de confianza del 95% “z “tiene un valor de 1.96

$$n = \frac{32\,(1.96)^2(0.5)(0.5)}{(32-1)(0.05)^2 + (1.96)^2(0.5)(0.5)}$$

n= 30

Anexo H. Preguntas para elaborar el código y las responsabilidades éticas.

Según COBIT 5 (2012) y las normas ISO 26000 y 37010 es necesario cambiar la cultura de la organización y tener identificadas las siguientes preguntas a la Organización.

1. ¿Quiénes son mis clientes internos y externos?
2. ¿La Institución está comprometida con la Gestión ética?
3. ¿Qué valores promueve la institución?
4. ¿Qué objetivos tiene la institución?
5. ¿El personal está alineado a los objetivos y valores de la institución?
6. ¿Cuánto riesgo siente la empresa que puede absorber y cuanto riesgo está dispuesta a aceptar?
7. ¿Hasta qué punto la gente acepta y / o cumple las políticas?
8. ¿Cómo trata la institución los resultados negativos, aprende de ellos e intenta corregir o serán asignadas culpas sin el tratamiento de la causa raíz?
9. ¿Identificar actos de corrupción y sus respectivas sanciones?

Para el correcto funcionamiento del código de ética es necesario constituir un Comité ético que realice constantemente la monitorización, valoración, modificación y aplicación de normas. Este comité tiene las siguientes obligaciones:

Comunicar a toda la empresa los comportamientos deseados y los valores corporativos.

Cambiar la cultura ejemplificando los comportamientos deseados desde la Gerencia y Jefes de mayor cargo.

Incentivos para fomentar y elementos disuasivos para hacer cumplir el comportamiento deseado, aplicar sistema de recompensas.

Reglas y normas, las cuales proveen una mayor guía sobre el comportamiento deseado (Código de ética).

Velar por las sanciones cuando se infrinja las reglas.